

To What Extent Has Information Security Professionalism Achieved Recognition?

A thesis submitted in partial
fulfilment of the requirements
for the degree of Doctor of Philosophy

Richard Phillip Reece

De Montfort University

December 2016 (Approved July 2017)

Abstract

The practice of securing information was until recently associated strongly with securing the Information Technology systems which store and process it. As it has developed as a specialised area of work however, particularly as the critical importance of human and social factors has increasingly been recognised, it has acquired an identity separate from that of computing. The separation has been sufficient for the formation of a new, distinct occupation, with specialised credentialing bodies being established to attest to practitioners' professional competence.

This study is the first empirical academic investigation into the professionalisation of UK Information Security. It considers attitudes towards professional status, the desirability and practicality of licensing, the current standing of the occupation and its prospects for the future. The analysis draws heavily from the substantial Sociology of the Professions, both from the structural and procedural theory of profession-forming and the later critiques of motivation, class and power. Semi-structured interviews were undertaken with twenty-seven individuals comprising security analysts, managers, academics, professional bodies and the UK Government. Interviews took place between November 2012 and March 2015. Results are presented in two stages of analysis, using Actor–Network Theory as a theoretical lens.

Whilst significant progress has been made towards forming a recognisable Information Security profession, its status is not yet comparable to more established peers. Aligned with US National Research Council findings but using a broader basis in professionalisation theory, the UK occupation was found to be too diffusely demarcated both internally and with respect to its bordering professions. It has yet to coalesce around distinct internal specialities with discrete qualification routes and establish the hierarchical arrangement of its major branches. Without such stratification of roles and a well-accepted claim to controlling a clearly demarcated body of knowledge, it is not possible to establish the boundaries of a graduate profession superior to any supporting para-professions, and thus position itself as requiring an advanced abstract education comparable to its peers. A rationalisation of credentials and institutions is required to produce a strong professional body which can advance the cause of the profession and properly establish and embed these roles. At present however – contrary to the tenor of much of the relevant sociology – neither the pursuit of professional status nor the exclusion of unqualified workers were found to be major motivators for current practitioners. By contrast government, the final arbiter of professional monopoly, is attempting urgently to increase the appeal of the profession to address a national skills shortfall, but is wary of direct market intervention in the form of licensing. Therefore, whilst change is rapid, significant impediments to full professional recognition remain.

List of Related Publications

Reece, R. and Stahl, B. (2015) “*The Professionalisation of Information Security: Perspectives of UK Practitioners*”, *Computers and Security*, Vol. 48, pp.182–195.

Acknowledgements

My greatest and first thanks must of course be to Professor Bernd Carsten Stahl, who from the initial exploratory interview onwards has been a constant source of good-humoured and helpful support, and without whose generosity of his extremely limited time and his great patience the entire project would not have been possible. I am hugely grateful that Bernd was able to act as first supervisor for the vast majority of the project and as co-author of the paper which arose from this work.

Alongside Bernd, I must record my sincere thanks to many other members of the De Montfort University staff who have rendered indispensable professional and personal help: Dr Iryna Yevseyeva, for her advice and support as second supervisor during the critical period of crafting the dissertation itself, and Dr Yingqin Zheng (now of Royal Holloway, University of London), who as the first supervisor during much of the first year of the project contributed greatly to setting me along the correct path and directing my early reading in subjects outside my previous academic training. Amongst her other contributions, I must thank Yingqin for introducing me to Actor–Network Theory and the philosophical work of its major proponents. I am also indebted to Professor Tim Watson (now of Warwick University) for his years as second supervisor and his introduction to many of the key contacts who contributed to the project either directly or indirectly. From outside the supervisory team, whilst many of the staff gave of their time and talents, I should note in particular the help and encouragement of Dr Helge Janicke, who acted as an independent assessor of progress on several occasions and made a large number of helpful comments and suggestions on each occasion.

Whilst all fees and expenses for the work were met personally, I must record (formally for disclosure but with all due gratitude) the contribution of paid study leave amounting to 98 days by my employer Airbus Defence and Space Ltd., whilst noting that their contribution was for my development alone and thus all opinions and conclusions in this dissertation are not ascribed to nor necessarily shared by that institution. In particular I would like to note the efforts of Kevin Stanley, Gareth Davis and Claire Roberts who were instrumental in granting the leave as well as being hugely supportive personally.

Obviously I must thank the twenty-seven volunteers who agreed to be interviewed, many holding very senior positions in multinational companies, universities, professional bodies and the UK government, whose time is extremely valuable. The contributions of these individuals,

although for obvious reasons anonymous, were in each case a profoundly generous and altruistic contribution to the advancement of the understanding of their profession.

I have been the extremely fortunate recipient of relevant professional expertise and assistance from amongst my personal friends. Chief of these, I would like to express my thanks to Dr Matthew Andrews, erstwhile Chair of the Association of University Administrators Board of Trustees. Dr Andrews was a source of very helpful expert advice and background information concerning the genesis and sustainability of university courses as well as encouraging me to consider undertaking the entire process. I am profoundly grateful to Miss Sophia Anderton, both for professional advice from her career as editor of several prestigious academic journals particularly during the preparation of the paper produced from the work, and for committing so much of her time to eradicating some of my typographical errors. I am also much obliged to Dr Lisa Mackenzie, Consultant in Emergency Medicine, for much informal discussion concerning the modern reality of working as a UK medical professional, providing crucial insight to the training and socialisation of the archetypal profession as practised today.

Finally I must acknowledge the huge debt owed to my wife Sarah for expressing no hesitation in allowing me to start this project, and for the time, expense and other sacrifices my family have made to allow me to pursue it.

Table of Contents

<i>Abstract</i>	<i>ii</i>
<i>List of Related Publications</i>	<i>iii</i>
<i>Acknowledgements</i>	<i>iv</i>
<i>Table of Contents</i>	<i>vi</i>
<i>List of Figures</i>	<i>viii</i>
<i>List of Tables</i>	<i>viii</i>
<i>List of Acronyms</i>	<i>ix</i>
 Chapter 1: Introduction	 1
1.1 <i>Information Security</i>	1
1.2 <i>Profession</i>	1
1.3 <i>Research Questions</i>	3
1.4 <i>Actor–Network Theory</i>	3
1.5 <i>Structure of the Dissertation</i>	4
 Chapter 2: Literature Review	 6
2.1 <i>Introduction</i>	6
2.2 <i>Information Security</i>	6
2.3 <i>The Sociology of the Professions</i>	22
2.4 <i>The Information Security Profession</i>	40
2.5 <i>Summary and Statement of the Research Questions</i>	49
 Chapter 3: Theoretical Basis	 52
3.1. <i>Introduction and Glossary</i>	52
3.2. <i>Prior Trends</i>	56
3.3. <i>Selection of Theoretical Perspective</i>	57
3.4. <i>Actor–Network Theory</i>	61
3.5. <i>Controversies: Sources of Uncertainty</i>	64
3.6. <i>Moments of Translation</i>	66
3.7. <i>Success</i>	68
3.8. <i>Criticism</i>	69
3.9. <i>Actor–Network Theory in Information Systems and Security Studies</i>	70
3.10 <i>Summary</i>	71
 Chapter 4: Methodology	 75
4.1. <i>Introduction</i>	75
4.2. <i>Data Gathering Methods</i>	75
4.3. <i>General Factors Affecting Methodological Selection</i>	87
4.4. <i>Data Gathering: Summary</i>	92
4.5. <i>Data Analysis and Coding</i>	95
4.6. <i>Research Plan at Outset</i>	99
4.7. <i>Execution of Research Plan</i>	99
 Chapter 5: Conceptual Analysis	 110
5.1. <i>Introduction</i>	110
5.2. <i>Housekeeping and Interview Administration</i>	110
5.3. <i>Personal Aspects</i>	111
5.4. <i>Certifications</i>	116

5.5. <i>Professionalism</i>	134
5.6. <i>Work Context</i>	145
5.7. <i>Summary</i>	168
Chapter 6: <i>Secondary Analysis</i>	170
6.1. <i>The State and Stability of the Current Network</i>	171
6.2. <i>Roles Within the Profession</i>	178
6.3. <i>Preparation for Practice</i>	184
6.4. <i>Professionalisation, Licensing and Regulation</i>	191
6.5. <i>Summary</i>	198
Chapter 7: <i>Conclusions</i>	200
7.1 <i>Answers to the Research Questions</i>	200
7.2 <i>Theoretical Considerations</i>	205
7.3 <i>Implications for Practice</i>	208
7.4 <i>Contribution to Knowledge</i>	209
7.5 <i>Limitations</i>	209
7.6 <i>Recommendations for Further Work</i>	210
References	212
<i>Appendix 1: Interview Instruments</i>	239
<i>Notes for Participants</i>	240
<i>Interview Protocol</i>	248
<i>Appendix 2: Coding Frame Details</i>	263
<i>Appendix 3: Interview Codes and Details</i>	270
<i>Appendix 4: Transcription Rules as Used</i>	272

List of Figures

1	Common computing career flows (from Bond, 1975).	8
2	A simple example of competition between existing professions relating to this study (examples given are purely for argument), based on the Abbot (1988) model.	33
3	A hypothetical example of Abbott splinter-based formation of a new group from amongst existing professions.	34
4	Subjective–Objective dimension (from Burrell and Morgan 1979, p.3).	54
5	A model of four sociological paradigms (from Burrell and Morgan 1979, p.22).	55
6	Illustration of OPP formation, from Callon (1986, pp.206–207).	67
7	Credentialing institutions as a possible “Obligatory Passage Point”.	72
8	Comparison of the “basic” research designs, from Flick (2009, pp.127–145).	79
9	Potential relationships explored in some potential case studies.	81
10	Key to later network fragment representations.	114
11	Derived network fragment observed in the certification market.	114
12	Network fragment observed with respect to academic qualifications.	120
13	Network fragment observed with relation to GCHQ accreditation of master’s degrees.	122
14	Network as inferred from the perspective of the practitioner.	130
15	Modified network seen from the perspective of the practitioner.	131
16	Credential network from the perspective of the practitioner.	134
17	Representation of a partial traditional professional status network (unified body).	135
18	Representation of professional status as the nexus of a partial network.	136
19	Partial view of an orthodox model of professional status.	141
20	Network instability caused by dissent to restrictions from security policy.	155
21	Potentially peer-symbiotic relationship between security manager and technician.	161

List of Tables

1	Regulation–Radical Change dimension (from Burrell and Morgan 1979, p.18)	55
2	Comparison of positivist concepts with anti-positivist analogues	88
3	A summary of candidate methods following the initial filter	93

List of Acronyms

(ISC) ²	International Information Systems Security Certification Consortium
ANT	Actor–Network Theory
BCS	British Computer Society
BERR	[UK Department for] Business, Enterprise and Regulatory Reform
CAQDAS	Computer-Aided Qualitative Data Analysis Software
CESG	Communications–Electronics Security Group
CPHC	Council of Professors and Heads of Computing
CREST	Council of Registered Ethical Security Testers
DBIS	[UK] Department for Business, Innovation and Skills
DCMS	[UK] Department of Culture, Media and Sport
DoD	[US] Department of Defense
DoHHS	[US] Department of Health and Human Services
DoHS	[US] Department of Homeland Security
GCHQ	Government Communications Headquarters
IISP	Institute of Information Security Professionals
ISACA	Information Systems Audit and Control Association
IS	Information Systems
IT	Information Technology
(N)CISSE	([US] National) Colloquium for Information Systems Security Education
NCSC	[UK] National Cyber Security Centre
NICCS	[US] National Initiative for Cybersecurity Careers and Studies
NRC	[US] National Research Council
NSC	[US] National Security Council
NSTISS	[US] National Security Telecommunications and Information Systems Security
OPP	Obligatory Passage Point
PC	Personal Computer
STEM	Science, Technology, Engineering and Mathematics

Chapter 1: Introduction

1.1 Information Security

The security of information has been a critical topic since antiquity. Julius Caesar's use of his eponymous substitution cypher (Suetonius Tranquillus 121, s.56) is perhaps the most famous illustration of ancient communications confidentiality, but is by no means the earliest example. It is probably since the advent of mass internetworking and ubiquitous processing of personal and corporate data however that Information Security has gained its modern prominence and significance. Information has long been liberated from behind a physical perimeter; the modern enterprise demands secure constant access to its data, as do its customers, partners, regulators and myriad other parties, at any time or place convenient to them.

At one point, keeping that information secure principally involved maintaining confidentiality, but no longer. Today there is no choice but to balance connecting to the rest of the world – with its attendant risks – against the certainty of commercial disadvantage from remaining unavailable. Furthermore, as the impact of failing to protect information has increased, a panoply of standards, regulations and statutes have come to shape the practice of *ensuring* that protection. Whilst the technical actions of defending against and forensically investigating such attacks are still vital aspects of practice and continue to evolve, to these have been added a new raft of activities. The modern enterprise boasts governance structures, processes for policy creation, awareness training, assurance auditing and so on. Understanding and developing all the factors involved has thus become the preserve of specialists.

Both history and sociology have much to say on the formation of new occupations. Occupations, if they sufficiently resemble knowledge-based, self-governing trades may graduate into “professions”, with consequences for the practitioners, their clients and society as a whole. The central question of this study is to what degree this has occurred in the field of Information Security.

1.2 Profession

The nebulous concept of “profession”, and the mechanisms by which groups sought and gained control over practice in an area of knowledge, fascinated and frustrated sociologists from the early twentieth century onwards. The early search for a definition bore poor fruit, producing only lists of traits seen in established professions, who themselves began only recently to

resemble today's concept of an ethical and qualified worker. Any hopes of a positivist empirical test arising from theory to separate occupations into "the professions" and "others", were eventually abandoned.

Whilst that early work is highly useful when identifying evidence of a campaign to professionalise an industry, the later more critical work is equally an essential foundation for placing this study in its proper context. Professions which obtain monopoly of practice control a market for work, and since they are frequently in high demand from paying customers they have developed significant wealth and influence in society. Sociologists therefore became more concerned with – and critical of – the motives and behaviour of these groups. Were their claims of disinterested practice and highly-educated expertise well-founded? Was it truly necessary to grant monopoly to an upper-middle-class cartel in league with the very top layers of society to the exclusion of others? This era, led by the prolific Eliot Freidson (e.g. 1970) but perhaps crowned by the (1977) work of Margali Larson, provides the background to why nation states have been so reluctant to grant licensing powers unless absolutely necessary, and hence the obstacles faced by a new candidate profession.

It is however the later (1988) work of Andrew Abbott which highlights the dynamic nature of profession-forming and competition between existing groups for the control of new ground. Abbott shows that far from being static entities immutably fixed into society, professions and their governing bodies are the product of dispute, negotiation and border conflicts with rival occupations in a constant struggle to maintain control of current areas of knowledge whilst competing for jurisdiction over territory opened by progress.

The literature review, then, establishes that the new field of "Information Security" (or increasingly commonly "Cybersecurity" although the former term will be used here) has emerged from its parent disciplines, and that it is a candidate to be considered amongst the professions. What it means to be a profession and the ramifications of that status are then considered, alongside how and why professionalisation of an occupation takes place. Prior work in the field is examined, particularly (2013) work by the US National Research Council on behalf of the US Government concerning under what circumstances the latter should consider "professionalising" the industry.

Whilst professionalisation has been painted merely as guilds self-interestedly desiring monopoly for private gain, the status and success of the Information Security profession has implications well beyond the welfare of its own members. As is reviewed in the next chapter and shown further in the later analysis, a combination of factors both technical and social have combined to produce the conditions where a rapid expansion of practitioner numbers and skills is required.

Whilst Anglo-American models of profession suggest a ground-up campaign for recognition by a sceptical state, by contrast the UK government is so concerned by the predicted shortfall of workers that it is itself taking active steps to catalyse the development of a “Cyber Security Profession” (DBIS, 2014). This unusual engagement extends not just into the education and certification of the profession but even to its *status*; the lure of other, more established career pathways dissuading technical graduates from entering a security career is listed as a principal cause of a skills shortage within the industry. That status therefore is in itself under scrutiny from those looking to drive the next steps in Information Security’s evolution. This study seeks not just to join this debate, but also to ground the discussion of these topics more deeply in a theoretical context from the substantial professionalisation literature than has typically been forthcoming from the existing work by national governments and industry bodies.

1.3 Research Questions

The literature review concludes that while there is evidence of professionalisation in Information Security, it is not yet clear to what extent this has been successful, what has caused or led this process, what its aims are and what if any obstacles remain. The following specific research questions are enumerated to state the current gaps in knowledge for these themes:

- What are the origins of the modern Information Security profession?
 - When and why did Information Security roles emerge and separate from Information Technology to form a new profession?
- What is the current status of the Information Security profession?
 - To what extent does a discrete area of practice exist with which the practitioners associate and what is its status?
- What are the prospects of further professionalisation?
 - Are there ongoing projects to professionalise the industry, what are their aims and are these being achieved?

1.4 Actor–Network Theory

The question of how and from what apparently stable social structures (such as professional bodies) are formed is the core of Actor–Network Theory (ANT). This approach is characterised by a symmetric treatment of human and non-human actors, in recognising that the “social world” comprises webs of interactions of both human and technical components to be considered even-handedly in judging their effect. Although based in earlier theory, starting with Callon’s (1986) paper its proponents emphasised accounts which describe how a focal actor establishes itself as the sole proxy or conduit for a desirable state for other actors, against a

background of competing actors seeking to do the same. Combined with its insistence that such arrangements are transitory and maintained rather than inherently stable and reified once created, and with Abbot's thesis mentioned above, it will be seen that this is an ideal lens through which to view the association of disparate elements into the beginnings of professional associations which compete for control of a highly technical area of knowledge.

1.5 Structure of the Dissertation

In the next chapter the literatures of Information Security and professionalisation are reviewed, followed by the existing work in the area of the Information Security profession. Having placed the subject in context and identified the specific research questions, a review of the applicable theoretical basis and its own literature is presented. This outlines concepts of ontology and epistemology and identifies the overall sociological paradigm which applies to the work using the model of Burrell and Morgan (1979). The selection is explained with reference to the nature of the work and the prevailing research traditions in the field. The principles of Actor–Network Theory and its particular suitability as a theoretical approach to this study are then set out.

The Methodology chapter comprises two major sections. The previous discussion of epistemology supports the identification of compatible methodological strategies, followed by the selection and justification of the specific data gathering method (semi-structured interview) and the overall research plan. Secondly, the execution of that plan is reported, laying out the work as actually performed and the sources of the obtained data, the deviations from the original plan, the issues experienced in the field and how the process of analysis was undertaken.

The analysis is presented in two chapters, which together form the bulk of the dissertation. Firstly the Conceptual Analysis sets out a description of and commentary on the data, organised according to the major codes from the categories created during the coding and annotation process. Secondly a more general second-stage analysis is presented, organised along the overarching themes which emerged during the study, leading to a number of conclusions. As Larson (1977) showed, professionalisation campaigns include an element of persuasion and campaigning; they must win subjective acceptance, not merely qualify against objective target traits however much they may resemble the behaviour of those who *are* so accepted. There is therefore no attempt to apply a binary “professional or other” model nor some quasi-quantitative ticking-off of a checklist against a set of metrics. Instead the analysis comprises a descriptive Actor–Network Theory account of the status, successes and failures of the professionalisation process to date and its subjects' future prospects.

Finally the Conclusion summarises the findings from the previous chapter and juxtaposes them

with the specific research questions to bring the study to a close, noting its limitations and how these might be addressed by future work.

To begin, therefore, it is necessary to review the literature to examine each of the two fundamental topics from which the rest of the work follows: what is Information Security, and what is a profession?

Chapter 2: Literature Review

2.1 Introduction

To put this study into context and establish a contribution to knowledge, it is necessary to survey the literatures of two disciplines¹. Firstly, by examining the history of Information Security itself, it is possible to trace its gradual separation from Information Technology into a discrete area of work. As this field is substantial, the aim is to highlight those themes which demonstrate how questions of risk management, governance, standards and regulatory compliance, policy and culture have created a discrete candidate profession. Any claim to professional status however must be grounded in an understanding of that term: what is a profession and why do occupations professionalise? Again, with such a vast field of work spanning nearly a century, the objective is to touch on those aspects which support the examination of professionalisation in an industry. The third area of review is the confluence of these themes: the Information Security profession itself. Whilst this area has been recently stimulated by government action, it remains a relatively new research domain academically. This chapter concludes therefore by summarising the opportunities for novel work and stating the research questions to be addressed.

2.2 Information Security

Information forms the heart of the modern enterprise, thus its protection is one of the key concerns of any organisation (Gordon *et al.*, 2003b). In the era of ubiquitous computing Information Security is virtually synonymous with the protection of data held in information systems (Wang, 1988). “Information Security” and “Cybersecurity” are sometimes used interchangeably, however to some the latter term includes protection of the *human user* as an intrinsic part of protecting their information (von Solms and van Niekerk, 2013). No distinction is made in this study but the former term is preferred, capitalised when referring to the area of professional practice or academic research under consideration here.

One definition for Information Security is given as:

“...protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.”

(Fuchs *et al.*, 2011)

¹ In doing so, this chapter includes material adapted from the paper linked to this study (Reece and Stahl, 2015).

Such statements are however descriptive rather than genuinely definitive, there being no well-established hard edge to the subject domain (Manunta, 1999); the certification provider (ISC)² for example includes at least a rudimentary treatment of physical security in its Book of Knowledge (Miller and Gregory, 2007) however this overlaps considerably with Corporate Security (Griffiths *et al.*, 2010; Coole *et al.*, 2015). The field has matured to comprise both technical and non-technical dimensions (Werlinger *et al.*, 2009; von Solms, 2001a; Brocaglia, 2005; Siponen and Oinas-Kukkonen, 2007; Bunker, 2012) through the abstraction of the practitioner from a role of computer data protection to that of governance (von Solms, 2006).

2.2.1 The Origins of the Information Security Occupation

The history of computer security is relatively brief and not extensively covered (de Leeuw, 2007; Greenwald, 1998), however *Information Security's* origins arguably begin with Spartan cryptography in the fifth century BCE (Kahn 1974, pp.67–71) since cryptography is included in the curricula of many of today's professional security certifications (White *et al.*, 2003; Miller and Gregory, 2007) although considered as mathematics by Siponen (2005). Cryptography was responsible for the simultaneous birth of modern computing and Information Security during the first automated attack on the Enigma system by the Colossus at Bletchley Park (de Leeuw, 2007).

Early computers were however single-user single-machine systems with little interconnectivity, thus their own security could be provided by physical protection of the equipment (Whitman and Mattord 2009, p4; Dlamini *et al.*, 2009). Following the development of multi-user systems, work was presented to the NSA in 1967 acknowledging the risk of information passing between users (Mackenzie and Pottinger, 1997), requiring *logical* security measures.

In military circles the scale of the computing security threat, and particularly the holistic technical and social response needed, was understood from early on (see Ware, 1970). Military work to protect independent tasks on mainframes resulted in formal access protocols such as the Bell–LaPadula model (Bell and LaPadula, 1973). Conversely, in the mainly educational civilian environment, protection of resources at that time was entirely optional (Mackenzie and Pottinger, 1997), particularly for commercial and home users (Greenwald, 1998). The advent of the Personal Computer (PC) in 1980 and later Apple Macintosh in 1984 introduced networks of small, single-user systems and pushed the computer into the hands of the untrained general public (Gollman 2011, p.4).

In early commercial computing the priorities were availability and functionality. No specialised security function was felt required (van Biene-Hershey, 2007); the field consisted almost

entirely of programmer and analyst roles, as can be seen in Fig. 1, reproduced from a trade newspaper.

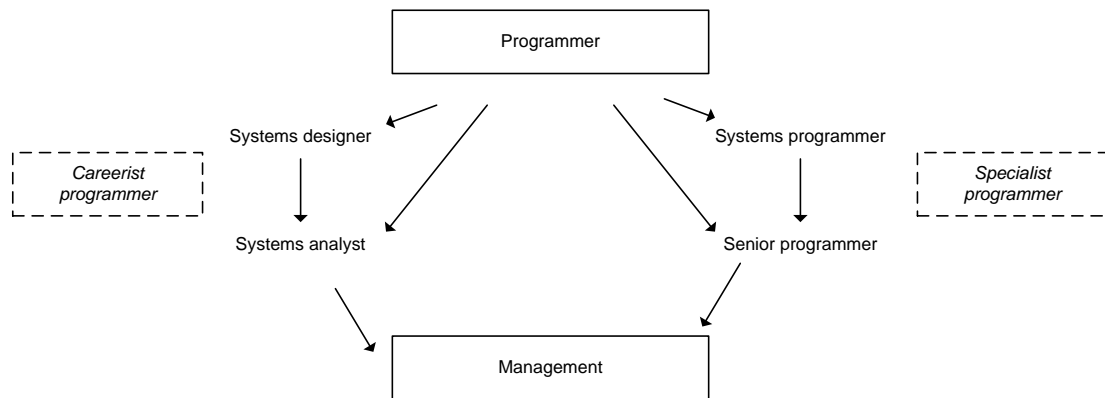


Fig. 1: Common early computing career flows (from Bond, 1975).

As computing became central to operations, security came to the attention of management (van Biene-Hershey, 2007) along with the requirement to balance user acceptance with secure practice, however security-minded analysts in the late 1970s were still struggling to gain acceptance of even basic password security (Morris and Thompson, 1979). Some future echoes can be seen however. Wooldridge *et al.* (1973) identify a role of a non-technical and senior “Security Officer” and devote a small chapter to its definition. Van Tassel (1972, pp.131–136) cites the importance of service bureaux separating clients’ data to avoid potential confidentiality breaches; a familiar topic for cloud computing today. One 1977 reference further suggests that the main principles of qualitative risk management were in use by this time (Courtney, 1977) which are reviewed later.

Moving to the 1980s, as the PC replaced the terminal, information systems research was turning its attention to IT management (Myers and Avison, 2002). Security was still not a real priority for management and few organisations supported a full-time manager (Straub, 1990). There is however some evidence of the *Security Consultant*. Talbot (1981) notes the corporate manager’s dilemma over whether to leave this important area purely to internal staff or seek external expertise from a specialist. In the same text there is also differentiation of *technical security tasks* and *security management*, noting that the manager must ensure that they remain in control of their assets but do not necessarily need to be technical experts to frame policy. “Management must manage. Actions can be delegated, responsibility cannot,” (p.13).

The security manager role which emerged in more advanced organisations had responsibility for policy, privacy, confidentiality and integrity (van Biene-Hershey, 2007). The role was a mixture of technical and organisational skills, able to understand the issues but also needing to

command respect within the organisation to be effective (Watt, 1989). Whilst security management became more common – Watt states that by the middle of the decade one was present in around 60% of organisations – this was typically at a junior level within IT.

In other enterprises security management at this stage was seen as a drain on profitability (Yost, 2015). Indeed, there is some evidence the position of security officer did not initially command professional respect as one might assume today. Watt (1989) states that it is “quite often ... thought of as the solution for the placement of an employee whose career may be ailing”. Christmas (1992), in a sister publication, allocated responsibility to senior IT and operational management streams and not to any defined security management function. This is somewhat curious, since the book is entitled “*Network Security Manager*”; possibly this specific role was considered a technical position. Such a world was ill-prepared for the advent of malware. In 1988 the first self-replicating computer virus was launched with devastating effects. The payload for this virus was simply the processing overhead of replicating itself, however the potential for damage had been proven (DeNardis, 2007).

In the 1990s the growth of personal and commercial internet usage put huge pressure on the still-new IT Security function (Dlamini *et al.*, 2009) which expanded strongly during the decade (Cresson-Wood, 1997). Viruses and hacking became a major problem for business (see Loch *et al.*, 1992), resulting in both technical security responses (anti-virus and firewall products) and personnel responses (social engineering awareness and behavioural training). The use of standards to structure proper security management became more common (von Solms, 1999).

“Ten years ago, information security policies were more or less unheard of outside the world of secret military and government IT networks. Now they are regarded by security professionals as one of the most important of the foundations of information security.”

(Lindup, 1995)

“The web” in the 1990s must be seen as a hybrid entity; the underlying connectivity, protocols, hardware and software had been in existence for many years; the significant change came during the mass uptake of the applications by the human user (Gollman, 2011). With the rise in online commerce came the opportunity for fraud, changing the focus of hacking from teenage prank to serious organised crime (DeNardis, 2007).

Moving into the new century, whilst the focus on IT Security has gradually increased, overall companies were still not resourcing the function adequately (Gordon and Loeb, 2002). PriceWaterhouseCoopers (2011) found that towards the end of the 2000s security funding had become stable and was maintained throughout the economic downturn, but that it was

vulnerable to ever-changing priorities. Compliance as a principal driver of spending tailed off after a peak caused by the Sarbanes–Oxley legislation (Johnson and Goetz, 2007), for example. Transitory management attention is a strong theme in the literature. Spending is often associated with specific events skewing perceptions of risk (Ezingeard and Bowen-Schrire, 2007) and hence proper Risk Management, which will be examined later.

2.2.2 Expanding Horizons: CIA and Successor Models

Information Security is frequently said to comprise Confidentiality, Integrity and Availability (“CIA”) (Brotby 2009, p6; NSTISS, 1994; Gollman, 2011; Posthumus and von Solms, 2004; von Solms and von Solms, 2008). This model is so well-entrenched that it bears scrutiny here before proceeding.

- Confidentiality refers to ensuring that information is available only to authorised parties, or “*the protection of information from exposure to others*” (Buche and Vician, 2005). Alongside concealment of information in transit through encryption, confidentiality requires the protection of stored data through access control, which requires authentication. Most users will be familiar with usernames and passwords, which become essential once remote access became available (Morris and Thompson, 1979), again bringing human factors into play. Passwords can usually be more easily compromised through social engineering against the human user than by technical attacks, particularly if policies do not respect the limitations of human memory (CESG, 2015; Alexander 2008, p.52; Adams and Sasse, 1999).
- Integrity similarly relies on good access control. “Information has integrity when it is whole, complete and uncorrupted” (Whitman and Mattord 2009, p.12). In other words, it is not sufficient for data to be available and private, it must remain reliable and correct to be useful. Freely available documents may still require protection against alteration depending on their use (NCSC, 1992). Malice is not the only threat to integrity; systems without inherent error correction are susceptible to alteration through fault or mistake (Humphreys, 2008; Whitman and Mattord, 2009).
- Availability (whether information is available to authorised users when it is needed) is often compromised in the pursuit of the two aspects above, but is just as vital. Besnard and Arief (2004) use the analogy of a car: at rest it is safe but also an expensive, useless object; the car must move (placing it and its occupants at risk) to actually function in any real sense as a vehicle.

Beyond “CIA”, since the expansion of e-commerce and computing in general, concerns now include *non-repudiation* and *accountability* (Brotby 2009, p.6; Whitman and Mattord 2009, p.9; Hamati, 2008; Siponen and Oinas-Kukkonen, 2007). Whitman and Mattord (2009) add Accuracy, Authenticity, Utility and Possession, although these are arguably augmentations of the original three. More generally however, narrow “CIA”-type classifications are inadequate if they over-emphasise individual threats and controls, but fail to include the social and ethical elements involved in the integration of the security management process into the organisation (Ashenden, 2008; Dhillon and Torkzadeh, 2006; Trompeter and Eloff, 2001).

Modern Information Security requires a holistic approach which includes the entire organisational infrastructure and staff (Bunker, 2012; Fink *et al.*, 2008). Demands for constant and wide-ranging information access from remote users who are able to distribute it further, give opportunities for misuse. To the original “CIA” aspects must therefore be added the (non-technical and traditional) qualities of Responsibility, Integrity, Trust and Ethicality (Dhillon and Backhouse, 2000). Modern security therefore places the human at the centre of its study.

2.2.3 An Overview of Human Factors in Information Security

Information Security concerns comprise technology, processes and people (Okenyi and Owens, 2007; Da Veiga and Eloff, 2007; Eloff and Eloff, 2003; Werlinger *et al.*, 2009). Technology has no pre-eminence; it is a tool available to both attacker and defender equally (Schneier 2008, pp.1–7). Of these, people are the least logical and predictable and the most likely to make errors; they are able to become dissatisfied, commit deliberate sabotage and are prone to external influence (Frangopoulos *et al.*, 2013). However, humans are also necessarily involved in any effective *solution*, through exhibiting secure behaviour and vigilance (Stewart and Lacey, 2012; Straub, 1990). Whilst implementing a security policy requires technical controls, these are not in themselves sufficient. Therefore, after a slow start (Cannoy *et al.*, 2006; Furnell and Clarke, 2012; Hitchings, 1995) security is now recognised in the literature as a multi-dimensional technical and human behavioural management discipline (Dhillon and Backhouse, 2001; Siponen and Oinas-Kukkonen, 2007; Ashenden, 2008; Ruighaver *et al.*, 2007; von Solms, 2001a; von Solms and von Solms, 2004; McFadzean *et al.*, 2006; Coles-Kemp, 2009; Besnard and Arief, 2004; Kayworth and Whitten, 2010; Soomro *et al.*, 2016).

The creation of a tailored and mission-appropriate policy, stating objectives and strategy rather than simply detailed rules and enforcement action, is a fundamental first step towards security (Blakley *et al.*, 2001; von Solms, 2001a; Doherty and Fulford, 2006; Stanton *et al.*, 2005; Baskerville and Siponen, 2002). Mere creation of a policy however does not lead automatically to acceptance, compliance and a secure state (Fulford and Doherty, 2003; Doherty and Fulford,

2005; Höne and Eloff, 2002b). Since they are as much instruments of internal power and control as a detailed statement of security principles and required behaviours (Stahl *et al.*, 2012), policy creation requires a negotiated process amongst several internal stakeholders (Flowerday and Tuyikeze, 2016). The security manager's organisational and diplomatic prowess therefore becomes as important as their technical knowledge.

Within the policy's scope and target, the "Insider Threat" remains a concern (Humphreys, 2008; Renaud, 2012) however it is perhaps now competing with other pressing topics for attention (Hovav and D'Arcy, 2003). Indeed, "*inside*" is now somewhat anachronistic (Leuprecht *et al.*, 2016; Palmer, 2005); networks became more porous as mobility dissolved the physical perimeter and network interconnection with partners and customers created hazy boundaries (Swindle and Conner, 2004).

Alongside malicious action, policy is challenged by non-compliance, wilful or otherwise. Human users of information systems have considerable freedom of thought and their own priorities for their interaction (Lamb and Kling, 2003). Where policies and controls disrupt or complicate operations there is clear incentive for users to circumvent them, at least where the cost of non-compliance and the effectiveness of any awareness training are not sufficient to counter this (Post and Kagan, 2007; Renaud, 2012; Bulgurcu *et al.*, 2010; Besnard and Arief, 2004; Furnell and Thomson, 2009; Straub, 1990; Albrechtsen, 2007; Thomson and von Solms, 1998; Thomson and van Niekerk, 2012). Similarly as security managers rarely have direct line control over the employees, they rely on local management to convey the importance and mandatory nature of the controls (Boss *et al.*, 2009), which may conflict with their own interests (Albrechtsen and Hovden, 2009). A policy which relies on execution by others must win their assent by some means, persuading the managers of key resources that it is in their interests to comply (Ashenden and Sasse, 2013; Johnson and Goetz, 2007), but assent (if won) strongly aids with gaining compliance (Albrechtsen and Hovden, 2010; Safa *et al.*, 2016).

Aside from questions of obedience, if writers do not sufficiently consider practicality and human limitations, policies and controls may become *impossible* for users to follow *even if motivated to do so* (Renaud, 2012; Sasse *et al.*, 2001). This has been erroneously addressed in terms of correcting the human "failure" however the failure point is not expecting humans to be fallible (Adams and Sasse, 1999; Dlamini *et al.*, 2009; Kraemer *et al.*, 2009) and failing to ensure that secure systems remain effective and useable for their function (Dhillon *et al.*, 2016). Compliance relies on human attitudes and habits: level and certainty of threat perceived, self-efficacy (confidence in one's ability to perform a task) and belief that the task is necessary and effective are highly relevant in persuading users to follow policy (Albrechtsen, 2007; Ng *et al.*,

2009; Vance *et al.*, 2012; Safa *et al.*, 2016). Moreover where the user can somehow justify their actions as necessary to perform their role or not damaging to the organisation (neutralisation) they will tend not to comply (Barlow *et al.*, 2013; Siponen and Vance, 2010; Hedström *et al.* 2011).

Internal education is often through *awareness campaigns*, however these are often unwisely structured top-down, assuming that technical content and the importance of compliance will be readily digestible and relevant to people whose primary roles are not security-related (Stewart and Lacey, 2012; Siponen, 2000; Guzman *et al.*, 2004; 2008). Better compliance is actually seen where the security function engages with the lived work of their clients in an involving and personally-relevant manner (Albrechtsen and Hovden, 2009; 2010; Siponen *et al.*, 2014; Puhakainen and Siponen, 2010; Fulford and Doherty, 2003).

Security comes from policy being accepted and lived as part of the organisation's day-to-day life (Thomson and von Solms, 2005) however today's newer workers were born knowing ubiquitous mobile internet access and powerful search engines, and for whom there is little boundary between work and home lives, therefore the challenge is to incorporate this mindset into company culture (Leuprecht *et al.*, 2016). Attempting compliance through pure disciplinary coercion, although partially effective if the threat is severe (Son, 2011; D'Arcy *et al.*, 2009; Herath and Rao, 2009a; 2009b) is not fully understood (Guo, 2013; Crossler *et al.*, 2013) and is rarely seen as the optimal strategy for gaining co-operation (Sasse, 2015; Kolkowska and Dhillon, 2013; Whitman, 2003; Vroom and von Solms, 2004; Ifinedo, 2014; Kankanhalli *et al.*, 2003). The security function if badly represented can appear to become a pure policing function and apparent antagonist for the user (Whitman and Mattord 2009, p.471).

To foreshadow the discussion of Actor–Network Theory, true cultural acceptance of security is where the desired behaviour is seen in the values of the staff because they have been enrolled in the security effort (van Niekerk and von Solms, 2010; Da Veiga and Eloff, 2010; Kolkowska and Dhillon, 2013). Instilling that security culture is the subject of a considerable amount of research, albeit empirically difficult to verify the effectiveness of a strategy. It is not proposed to explore this here – the interested reader may be directed to Karlsson *et al.* (2015) – it is simply necessary to note the importance of this topic for later argument. Rather than reifying security into a commodity to be bought, it is necessary to make the behavioural and cultural adjustments necessary to respond properly to the entire spectrum of threats (Stahl *et al.*, 2008).

2.2.4 Standards and Legislation

So far the internal choices and pressures for the security manager have been noted. There are

however several sources of externally-derived structured constraints on security practice, which vary significantly for intention and sanction but which together constitute *coercive isomorphism* (DiMaggio and Powell, 1983; Gerber and von Solms, 2008). These pressures may however actually empower the security manager and lead to greater internal resource allocation (Cavusoglu *et al.*, 2015). The degree to which organisations are subject to these influences depends on their market area, however even unregulated industries will be subject to general statutory controls such as data protection legislation, creating further pressure for security staff to master non-technical policy and compliance skills (Burdon *et al.*, 2016). In some environments the preponderance of regulation may even require a dedicated compliance officer to prevent private or corporate sanction (Freeman, 2007).

Standards are in theory merely instruments of compatibility; they embody agreements between interested parties on a common set of objective criteria for determining whether an item complies with a given specification. They are however created by an interest group for some motivating reason and when adopted translate the priorities of the author and adopter into internal compliance and policy action; they are also instruments of politics and power (Backhouse *et al.*, 2006), prescribing a common set of processes for all, often regardless of their individual circumstances (Siponen and Willison, 2009).

Adoption may be uncontroversial commercially, for example apparent non-compliance with PCI-DSS² may be unthinkable in retail industries. Similarly the ISO27000/BS7799 standard suite is a frequent cause of IT Security management formalisation in the twenty-first century due to its widespread adoption (Humphreys, 2008; von Solms, 2000). To preview the discussion of Actor–Network Theory, the real power of a voluntary standard comes when its adoption gathers momentum and displaces even potentially superior competitors through market share and general recognition (Heinrich, 2013). For less well-accepted standards, benefits may be less clear-cut (Johnson and Goetz, 2007), requiring security practitioners to prove (or rather sell) their commercial advantages to management. Similarly the pressure may well be to simply achieve *certification* for its own sake rather than truly accept and adopt its ethos unless the correct cultural change is achieved (Ruighaver *et al.*, 2007).

Data for which a company is liable are increasingly processed by others. Whilst it is sometimes a statutory duty to specify a standard contractually to the processor such as under Sarbanes–Oxley (Mahdavi and Elliot, 2005) to mitigate risks from mishandling, it is uncertain whether this genuinely ensures good internal security hygiene and robust protection of data (see

² Payment Card Industry Data Security Standard, mandatory for merchants processing card payments

Humphreys, 2008). It may simply provide a defence against criticism by complying with *due diligence* requirements. The content of the standard in the latter instance is then all but irrelevant, the material point being the act of adoption itself (Siponen, 2006), becoming a *black box* as will be discussed later.

Legislation is often broader than more detailed standards, and need not have computing systems as its focus; Sarbanes–Oxley for example requires the organisation to have effective controls, which compels a technical response internally (von Solms, 2006). In like manner, the Health Insurance Portability Act was the first US legislation to require standards to be set for protection of health-related data (US DoHHS, 2011). Enforcement action has raised compliance awareness (Grandison and Bhatti, 2010) catalysing changes which hitherto had been politically difficult to obtain inside organisations (Johnson and Goetz, 2007). Statutes however are difficult to keep current and relevant (Walton, 2006) therefore secondary legislation by regulations is often used. Similarly standards such as ISO27000, COBIT and similar models prescribe policies but avoid mandating detailed controls lest they become swiftly outdated (Höne and Eloff, 2002a).

Legislation has mandated changes to the industry itself. The US “Information Assurance Workforce Improvement Program” mandates minimum qualifications for assurance roles in the US Department of Defense (US DoD, 2010) thus driving the certification market reviewed later. The EU General Data Protection Regulations mandate a data protection officer (Tankard, 2016) but their full impact is not yet fully known.

2.2.5 Security Governance

In the sections above, the increasing complexity and decreasingly techno-centric nature of Information Security were seen. Von Solms (2000) initially characterised the development of Information Security into three phases (“waves”):

- Technical: Hardware is isolated, physical security and rudimentary controls are sufficient.
- Management: Security is a key task recognised by senior management, accompanied by the introduction of “policies, Information Security managers and organisational structures”.
- Institutionalisation: Realisation that the human was central thus creating a culture where secure practices are routinely included in the everyday work and custom of the average employee was necessary, rather than individual controls (see also Da Veiga and Eloff,

2007).

After a number of corporate scandals raised the profile of corporate governance, legislative responses such as Sarbanes–Oxley made directors personally liable for corporate failings, thus ensuring management attention (Dhillon and Mishra, 2008; Freeman, 2007). A “Fourth Wave” followed (von Solms, 2006) where security moved from an important part of IT management to an aspect of *corporate governance*. This is the point at which the security manager perhaps gained most prominence and – crucially – separation from the IT infrastructure. In the story of the Information Security profession therefore this is a critical turning point: responsibility has been passed to the board, but the board must in turn rely on specialist advice.

“[Governance is] the set of responsibilities exercised by the board and executive management with the goal of providing *strategic direction*, ensuring that *objectives are achieved*, ascertaining that *risks are managed* appropriately and verifying that the enterprise’s resources are *used responsibly*.”

(ISACA cited in Brothby 2009, p.5, emphasis original)

In other words, management aspects of Information Security practice may be labelled – in order to separate them from technical implementation and procedural controls – as “governance”, or the Information Security Management System (ISMS) (see Broderick, 2006). This refers to the organisational forms which manage not the actual movement of the information, but review and direct the mechanisms by which this is controlled. Through this, implementation of the required controls becomes *systematic* and aligned with the management of other business areas (Ashenden, 2008). The organisation must establish that it (verifiably) complies with all statutory and regulatory requirements, and standards of best practice (Calder and Watkins 2008, p.2) as a separate dimension from simple operations and performance management (Fink *et al.*, 2008).

Several models for information security governance exist and it is not proposed to review each in detail, since this has been done elsewhere and most relevant here is in the pressure they create rather than their exact composition. See for example the comparison by Da Veiga and Eloff (2007) of four prominent models (ISO27001, PROTECT, the Capability Maturity Model and Tudor) and their synthesis of a composite framework from them. Many other governance structures are similarly influenced by the ISO27001 or COBIT frameworks and mandate positions for specialist security staff; see Eloff and Eloff (2003), or the Calder and Watkins (2008) model which assumes an Information Security Manager and accompanying expert (but not exclusively technical) adviser. The recent model of Carcary *et al.* (2016) provides a maturity assessment substantially based on these standards.

Whereas technical controls are *implemented and operated* by operational staff, security strategy

sits squarely with the board to instigate and delegate down through an effective structure where appropriate. Many authors and standards stress this point (Barton *et al.*, 2016; Hu *et al.*, 2012; Puhakainen and Siponen, 2010; Neal, 2008; Knapp *et al.*, 2006; von Solms, 2001b; Fink *et al.*, 2008; Ezingard and Bowen-Schrire, 2007; Kankanhalli *et al.*, 2003), however McFadzean *et al.* (2006) provide a very useful summary of the rationale, paraphrased below:

- Without the authority of the directors, it is impossible to implement the controls required for adequate security and force compliance,
- Security must become a part of corporate culture, which can only be achieved by those who lead and create that culture,
- All enterprise risk management is the responsibility of the board because they are ultimately responsible to shareholders and regulators,
- Directors have the unique perspective which allows them to judge the value of information assets,
- The board's duty is to ensure the company remains competitive and therefore secure.

This creates the pressure to ensure good governance but not necessarily direct control of detail; directors are after all responsible for legal compliance and financial performance but are not all accountants or lawyers; executives direct, whilst policy is created in the management layer (Posthumus and von Solms, 2004). Boards must therefore create the conditions whereby technical decisions are organised and taken well, since many technical areas are simply “invisible” to them without professional guidance (Rainer *et al.*, 2007; McFadzean *et al.*, 2007) or which they will struggle to judge on an informed basis (Straub, 1990). This provides a foundation for Information Security as a distinct function.

The positioning of this function in the organisation is significant. There is no well-established single model for this (Cannoy *et al.*, 2006); security practitioners were historically found in IT reporting through the CIO (Ayoub, 2011; Johnson and Goetz, 2007) at least in part because of its origins as a technical discipline (Brotby 2009, p.1). Many practitioners will have come from non-security technical backgrounds; refusal to acquire the additional skills and attitude required to broaden competence creates a *de facto* glass ceiling (Brocaglia, 2005; E-Skills UK, 2013). The effects of technical controls however (and particularly any failure of them) are still one of the security team's most visible “products” within an organisation.

Neal (2008) identified three broad types of security management role distribution in orthodox hierarchies:

- No formal security manager exists. Technical functions are carried out, potentially in isolation, by individuals in technical groups. Responses to technical threats may be mitigated however there is a lower emphasis on policies and standards.
- A role is established with responsibility for policy, procedure and disaster recovery but without direct authority over implementation.
- A formal CISO figure exists with direct prescriptive authority over technical security specialists, possibly through line management authority.

Neal's (2008) suggestion that these types represent an evolution linked to size through simple division of labour is in principle reasonable: unless there are sufficient numbers of security employees the management, technical and non-technical roles cannot be separated and split hierarchies formed. The main sources here cannot assist in this enquiry; purely data-driven demographics studies (such as E-Skills UK, 2013), whilst producing useful information on certification and age data for example, are rather unsatisfying in delivering conclusions which are theoretically interesting since they lack any context to the decisions and choices represented. Qualitative, exploratory work would be useful in this field.

More recently, it appears that security's reporting lines are increasingly to senior business management (possibly the CEO) as well as senior information management (Winder, 2009). A PriceWaterhouseCoopers (2011) survey showed that whereas in 2007 38% of principal security officers reported through IT, by 2010 this had reduced to 23% in favour of operational directors. This was attributed to an increasing appreciation by company boards that the protection of information assets was a business goal rather than a technology function.

Can IT Security management be positioned *effectively* within the IT hierarchy, given its regulatory or policing function? Hayes (2002) quotes two contrasting views from industry; one notes a potential conflict of interest between the policer and the policed, since a key role of IS security is one of audit, however the other sees reporting through the CIO as both a method to gain heavyweight management support and to introduce an expert champion able to understand the issues. Whitman and Mattord (2009, pp.28–32) place the CISO role as a direct report of the CIO, seeing security as a function of the IT department. Even in larger organisations there may even be intervening management, suggesting that this is not a form of "CxO" top leadership role implied by the word "Chief" which to some will devalue the position (Brocaglia, 2005). It is

important that the role tasked with audit or risk assessment is not placed too low in the organisation however since this will lead to judgement being affected by internal political pressure from operational management. The needs of a production department may be at odds with security requirements, it might be possible to bring a system into production more quickly if security controls are not imposed (Alexander 2008, p.17; p.114).

2.2.6 Risk Management

Risk Management is central to security governance and therefore effective modern security practice (Dhillon and Backhouse, 2001; von Solms and von Solms, 2008; Wang, 1988; Whitman and Mattord, 2009). It has gained particular prominence since the rise of governance structures (von Solms, 2006) and continues to increase in importance (DBER, 2008) reflecting the increasingly information-dependent nature of the modern enterprise (Gerber and von Solms, 2001). The assessment and balance of competing factors required is important for the claim of security management as a relatively non-technical business-centred area of professional judgement and thus part of a discrete area of work.

Risk Management is the systematic enumeration and evaluation of the likelihood and impact of potential undesirable events and devising a strategy for accepting or reducing each within an overall tolerance for uncertainty or “risk appetite”. It requires judgement to implement, since absolute protection of every asset is unnecessary and unprofitable if not impossible (Campbell *et al.*, 2003; Brocaglia, 2005). It forms part of an effective governance programme, to identify unacceptable risks and design a response to the principal threats (Straub and Welke, 1998).

Security exists within corporate commercial reality; just as accountants cannot refuse to spend any money, security managers must balance risk against restraining productivity, otherwise products cannot be brought to market and the business will fail (Neal, 2008). Consequently the function must understand the mainstream business to contextualise their judgement, establishing interfaces with enterprise senior management (Rainer *et al.*, 2007; Fitzgerald, 2007). Security incidents are an inevitable cost of operations, which can be reduced to some extent by optimising security spending to reduce that loss (Fink *et al.*, 2008; Gordon and Loeb, 2002; Campbell *et al.*, 2003; Brotby 2009, p.2). To do so, security must understand each area of the business in order to identify weaknesses before they are exploited (Mahdavi and Elliot, 2005; Raywood, 2012). They must be able to understand the business impact of information loss to judge how much effort to expend towards its avoidance (Bunker, 2012).

The risk manager is not a system owner, they are a consultant in its welfare and their advice must be fully aligned with the organisation’s strategy and goals (Foster, 2005; Johnson and

Goetz, 2007). They must display a positive attitude as an enabler rather than a preventer (Brocaglia, 2005). Ensuring that the function is (and is perceived to be) opportunity- and business-led is crucial to the inclusion of the security function during the development of strategy. Prior to security moving out from technical obscurity, business managers deliberately avoided engaging and requesting advice as the answer tended towards the restraint of novel ideas or greater flexibility; such a conservative and restrictive model is no longer sustainable (Moritz, 2005). The CISO must ensure that security strategy is aligned with both IT and corporate strategies (Seeholzer, 2012). Attitudes to security are heavily dependent on market context; agility is still the over-riding priority for organisations in fast-moving sectors thus it is vital that risk analysis and security culture are aligned with the organisation's own major values and strategy (Johnson *et al.*, 2009).

Organisations naturally choose different attitudes to risk as another variable in normal commercial competition (McBride, 2005; McFadzean *et al.*, 2007). Strategies for exercising that choice vary; ISO27001 for example supports accepting the risk and factoring in its cost, avoiding it by somehow reducing the frequency of occurrence, transferring the risk outside (possibly to specialists in controlling it) or reducing the impact through some mitigating action (Humphreys, 2008; Blakley *et al.*, 2001). The security manager as risk assessor has a role in shaping enterprise strategy and must thus be able to advise senior management in business terms (Brocaglia, 2005).

A structured framework for dispassionate and regular *prior* assessment of risks is important (Cavusoglu *et al.*, 2015). Security policies which are created as counter-measures after the fact may be ill-considered and are rarely well implemented (Cannoy *et al.*, 2006). Corporate leadership however often requires some external impetus to take a direct interest in security matters (Ezingard and Bowen-Schrire, 2007; Doherty and Fulford, 2006). Outside such crises, risk decisions are frequently taken on the basis of unwarranted optimism in the assessment of the risk, partially due to the illusion of controllability (Rhee *et al.*, 2012).

Qualitative and quantitative variants of risk management exist; both estimate risk as the product of likelihood and impact, however they differ on how this information is assessed and what level of precision is claimed (von Solms and von Solms 2008, p.87). Quantitative approaches attempt to assign a *value* to the loss, often to calculate whether proposed discretionary security spending would represent a good investment (Gollman 2011, p.29). Qualitative methods by contrast classify risks into multi-dimensional strata based on impact and likelihood using either objective criteria or by simple assessment (White *et al.* 2003, p.486). An organisation can therefore rank risks to be mitigated or set a maximum score as a method for selective

acceptance.

The most widely-known quantitative model is *Annualised Loss Expectancy* (ALE), where the statistical chance of a scenario and the cost of its impact are multiplied to give an annual spend for that scenario, the sum of all such events representing the overall loss due to risk (Blakley *et al.*, 2001). This is of course only a simple model and ignores some relevant factors; some risks may not be *morally* acceptable to assess purely on financial costs for example, since there may be a social, personal or reputational cost of inaction which cannot be ignored (Courtney, 1977; Oppliger, 2015). Similarly *unsurvivable* impacts are terminal and thus prevent costs from being averaged out over the longer term, thus avoidance of these must be prioritised (Bodin *et al.*, 2008).

The principal criticism of quantitative measures is that the probabilities of many events cannot be predicted reliably since accurate occurrence data is not available (Oppliger, 2015; Anderson, 2003) and anyway will vary according to sector and resources available to respond to incidents (Humphreys, 2008). What data is available are often from badly constructed work or with poor levels of statistical analysis (Ryan and Jefferson, 2003). Similarly the reduction in occurrence for mitigating actions cannot be known accurately; it is challenging for example to calculate whether an action has deterred an attack (Stewart, 2012; Ryan and Ryan, 2006).

Gordon *et al.* (2003a) counsel using the enterprise's own experience for incidence and loss figures, however even if this data *is* well known, the impacts – particularly to such intangibles as reputation, morale and goodwill – are similarly problematic to predict accurately (Hovav and D'Arcy, 2003). Quantitative data is therefore in reality often estimated and the result somewhat subjective. Moreover even well-intentioned human nature can lead the author to err towards the value which is most convenient for their argument (Hovav and D'Arcy, 2003; Anderson, 2003) or use information from parties with an inherent interest in supplying the data (Stewart, 2012). The use of “objective” risks as a political lever for justifying extra resources is therefore noted as a point of interest.

Since an insurance sector is growing to respond to such risks it can be expected that work will continue on accurately gauging the financial impact of breaches (Johnson *et al.*, 2009) however this may only be practical for insurers with access to a substantial data set. Such efforts will be hampered by a general reluctance to publish security-related data due to stock market effects (Campbell *et al.*, 2003; Spanos and Angelis, 2016; Hovav and D'Arcy, 2003; Kotulic and Clark, 2004) however legislation in the US and EU should force companies to reveal this information (Tankard, 2016).

Quantitative analysis has the benefit of simplicity and clarity. Executives comprehend a three million dollar loss from bad publicity more readily than a risk rated as “16” (Miller and Gregory, 2007). Qualitative risk analyses however can be challenged where perceptions of risks vary from those presented. McFazdean *et al.* (2007) found that risk perception amongst senior managers varied greatly, even amongst those in apparently similar organisational contexts or business sectors. They posited that there was a continuum of “perceived risk” according to the individual’s own values and attitudes which, when combined with the degree to which the organisation’s use of technology was strategic, affected the stance of that organisation towards security spending and acceptance of controversial policy items. An ambitious security function in those organisations whose executives perceive the prevailing risk to be too low will therefore need to engage politically to alter those perceptions.

Much work has been undertaken in the area of risk metrics, both to improve the level of Risk Analysis (Anderson and Moore, 2007) and to aid the process of measuring compliance for assurance purposes (von Solms, 2001a). If risk management is the business of reducing risk to acceptable levels, is there a mechanism for translating the potentially subjective statements of risk appetite from the board into an objective set of criteria for what constitutes acceptability? There is the opportunity for this “mechanism” to be the security specialist.

In summary, security therefore is no longer a merely technical domain; it consists both of technical threats which can be quantified and systems configured to detect or prevent, and of less predictable and human-based aspects which must be understood and incorporated into a strategy of defence and awareness (Spagnoletti and Resca, 2008). The discipline finds material form in the policy document and organisational form in the ISMS. It includes operational details of policy enforcement but goes beyond them. Supporting this is the Information Security practitioner, a possible candidate profession. What then does it mean to be a “profession”?

2.3 The Sociology of the Professions

It was argued above that the emergence of Information Security had potentially created a discrete “profession”, therefore it is necessary to understand what this entails. Information Security workers have become a more active topic for researchers recently following government intervention, however this has rarely been linked with the study of *professionalisation*, which represents a very substantial area of twentieth and twenty-first century sociology. The sheer scale of work in this area defies ready summary, however the key history and theory of that discipline are reviewed below, in order to support the later stages of analysis.

2.3.1 Introduction

The principal *sine qua non* distinction of “the professions” in the modern age is work requiring a proven, advanced level of knowledge or education, however this is usually coupled to a commitment to ethical practice, some form of altruistic conduct, and regulation by a body of peers (Saks, 2012; Millerson, 1964). Beyond this, regional variations exist in concepts of “profession” and in the modes of their formation (Freidson 1986, p.13), thus in professionalisation studies it is necessary either to contrast these or work within a single cultural model. In keeping with the UK-centric scope of the overall study and the bulk of the English-language literature, the state-sponsored Anglo–American concept is the focus of this study, rather than the top-down state-imposed continental model (Neal and Morgan, 2000; Saks, 2015). European sociology has indeed sometimes regarded the British and American discussions as curious, since many non-Anglophone cultures have no equivalent concept (Sciulli, 2007). Some of this discrepancy may originate in European professions being mainly employed and controlled by the state whereas in the UK and US they are seen as more autonomous, however even this is not a clean comparison of types (Evetts, 2003).

Professionals became identifiable once university degrees distinguished priests, physicians, and lawyers by higher levels of general learning through *liberal education* (Crook, 2008). Universities themselves were originally influenced heavily by the Church and in many cases even secular professions were originally comprised mainly of those in orders (Goode, 1960). Indeed, the etymology of “profession” is related to the monastic act taking of a sacred vow (Freidson 1986, p.21).

It is no coincidence that professions are linked with status; when livings were made from the land and indivisible estates entailed as a self-supporting entity to a single scion in turn, an income and purpose was needed for any younger sons. Careers with suitable status and income were not readily available and appointments made by patronage rather than on merit (Reader 1966, pp.2–10). The industrial revolution however created a wealthier middle class, able to pay for professional services but with less control over the professional’s work, given their new wider source of potential clients (Johnson 1972, p.52).

Thus our society inherits “the professions” as an apparently ancient concept. In reality however, that concept has evolved with the rest of society. Medicine, as one would now recognise it, is for example far more recent than the foundation of the Royal College of Physicians under Henry VIII in 1518 (Saks 2015, p.27). Despite its long history, a recognisable unified occupation (formed from apothecaries, surgeons and physicians, with the druggists distinct in the Pharmaceutical Society), undertaking ethically regulated practice with systematic education and

legally-enforced training was not present until at least the late nineteenth century, following the passage of the Medical Act 1858 (Reader 1966, p.41; p.67), and arguably later still. What then is a profession and why does its definition allow such leeway?

2.3.2 Traits, Definition and Function: Division of Labour in an Ordered Society

“To define profession is to invite controversy.”

(Cogan 1955, p.105)

Whilst professions are hugely significant for both citizen and corporation alike, representing some of society's most powerful and influential entities (Abbot 1988, p.1), it is not clear precisely how a profession truly differs from any other occupation. A profession, as understood in earlier studies, is an occupation whose competent undertaking is important; it is considered at least partially altruistic and a valuable service to society, or “good” work (Freidson 1994, p.200). It requires substantial, abstract knowledge learned as theory, which is then combined with judgement and practical skills to be applied to the particular situation of a client in an ethical manner, to a standard acceptable in the eyes of their peers; standards are typically maintained through membership of an institution which issues credentials and can revoke these for misbehaviour or incompetence (Millerson 1964, pp.148–180). Since the professions typically handle sensitive information and the vital interests of their client (Evetts, 2013), their probity must be beyond question (Reader 1966, p.159); where the state has been persuaded that *sufficient* risk is associated with incompetent or unethical practice and hence *caveat emptor* is not desirable (Larson 1977, p.49), *and* that there exists a body which can regulate it and agitates for that (Freidson 1986, p.35), membership of this institution becomes mandatory and the professionalisation process (or “project”) is complete.

As a result of the training, knowledge and ethical standards achieved (and responsibility which flows from technical autonomy) the profession is usually granted high status by society and frequently able to charge a high fee (Cogan, 1955; Gorman and Sandefur, 2011; Freidson 1994, p.200; Sciulli, 2007; Macdonald 1995, pp.157–171). The degree to which practitioners had associated, organised themselves and claimed monopoly over their areas of expertise was once seen as a continuum on which all professions could be placed, assessed by case study (Abbott, 1988; Gorman and Sandefur, 2011; Greenwood, 1957). The full profession then is at heart a bargain: the state awards control – over an area of knowledge so complex and esoteric that competence can only be judged by peers – to an organisation of practitioners in exchange for accepting responsibility to ensure that it is competently and ethically performed (Susskind and Susskind 2015, p.23; Freidson 1986, p.33).

The attempt to create a taxonomy of profession is often divided into the trait model – what specific behaviour, characteristics or properties mark out professions from other occupations – and the functionalist model– what function do they fulfil in society. The trait model could be seen as the positivist aspect of the field, concerned with developing a basis for empirically determining professional status (if criteria could be established), or even the degree of professionalisation if one assumes a calculable metric. The earliest attempt to establish an analytical literature is usually credited to the substantial (1933) trait-based work of Carr-Saunders and Wilson (Abbott 1988, p.4; Freidson 1986, p.27; Crook, 2008) who surveyed around thirty professions, almost entirely still extant and generally recognised (pp.7–288) followed by a comparison of the similarities and differences between them.

This was the start of a period of many such analyses and lists of criteria. Cogan’s (1955) attempted definition is typical:

“A profession is a vocation whose practice is founded upon an understanding of the theoretical structure of some department of learning or science, and upon the abilities accompanying such understanding. This understanding and these abilities are applied to the vital practical affairs of man. The practices of the profession are modified by knowledge of a generalized nature and by the accumulated wisdom and experience of mankind, which serve to correct the errors of specialism. The profession, serving the vital needs of man, considers its first ethical imperative to be altruistic service to the client.”

(Cogan, 1955)

Millerson however both created such a set of criteria and immediately challenged the concept. His list itself is similar:

- “a profession involves a skill based on theoretical knowledge
- the skill requires training and education
- the professional must demonstrate competence by passing a test
- integrity is maintained by adherence to a code of conduct
- the service is for the public good
- the profession is organised”

(Millerson 1964, p.4)

Millerson himself notes however that these are descriptive of an *ideal type*; since even medicine has not always possessed all of the above therefore they cannot be considered *essential*. The distinctions identified were rarely theoretically-based, often being a simple retrospective deconstruction of the claims of existing dominant professions (Mangan, 2014). Furthermore, as Millerson goes on to show (1964, p.7), taking atheoretical assumptions that professions must

resemble prototypes leads to problems when work takes these as *qualifying* criteria. For example, the concept of deprofessionalisation (that professions have lost some essential component by moving from autonomous practice in small cells of practice to controlled work in managed bureaucracies) is based on acceptance of that autonomy as a criterion, however that acceptance is merely observational with little basis in an accepted “general theory” of the professions.

In search of alternative models, Susskind and Susskind (2015, p.15) cite the Wittgensteinian analogy repeated by Downie (1990) of four brothers sharing similar characteristics without being clearly identical. This is an alluring but unconvincing comparison, since fraternal similarity has an *external rationale* for the selection criterion, whereas to select on the basis of similarity without a theoretical basis and then define by that similarity is surely not a useful taxonomy for many purposes.

Ultimately therefore this attempt to create a strict definition of a nebulous concept by trait was unfruitful. More successful were functionalist descriptions of their role in society. Society needs to control that work which results in damage if performed badly, but is corporately inexpert, thus those with equivalent specialist knowledge must do the judging (Rueschemeyer, 1983). Altruism for example, is seen here as not simply a *trait* but as a useful *function* in the ordering of society (Saks, 1995, p.15). Functionalists such as Parsons and Goode (e.g. 1960) looked for the essentials of a professional’s practice in its work context (Johnson 1972, p.37) and were granted their status in exchange for diligent execution of important and responsible work (Saks, 2012).

These earlier analyses tend to assume that professions are both clearly distinct in some manner from other occupations (Johnson 1972, p.10) and positive for society (reflecting their contemporary high social standing), seeing them as moral bulwarks in the maelstrom of social life and guards against an interfering state (Macdonald 1995, p.2; Johnson 1972, pp.21–38; Millerson 1964, p.220). This can be overstated however and even in the early work there is acceptance of the possibility of self-interest (Saks 1995, p.16; Parsons, 1939) and a risk acknowledged in granting monopoly (Carr-Saunders and Wilson 1933, p.1). As will be seen below, even the relatively unquestioning early acceptance of the claims of professions to be a force for social good were short-lived. As the concept of profession is malleable according to the prevailing ordering of society, so is the attitude of its critics to its central claim: altruism.

What then of a definition? Simply, *if* it is possible for professions to be described from a theoretical basis, it has not yet occurred. In any case to be a profession involves subjective recognition not simply objective compliance with some criteria (Millerson 1964, p.9). As

Bennis (1973) noted, the act of even questioning one's own professional status is a sign of insecurity and thus presumably a professional project which is not yet complete.

For some, establishing an exact definition is simply not important; the search for a precise definition is an unhelpful distraction (Evetts, 2003; 2006). For others (for example Freidson 1986, p.30) it is essential when drawing and comparing analyses of phenomena to ensure that all parties are comparing like concepts and are agreed on the scope and nature of the object studied, since the only practical alternative is for each to use their assumed working definition which remains unchallengeable. Moreover if you make an arbitrary choice of a certain subset of candidates without foundation, such as defining professions by their power or influence – as many did, for example Johnson and Freidson respectively – it surely becomes circular to then describe the attainment and abuse of power of professions as being *inherent* to the class. Others reflect the later, pragmatic position that a strict definition is unnecessary; provided that the writer can identify a subject and apply his chosen theory to it (Abbott 1988, p.318; Evetts, 2013) no further precision is necessary, given that there is “general agreement” about what constitutes a profession (Larson 1977, p.x).

There must be careful treatment of motive; status descriptions, as writers such as Macdonald (1995, p.3) describe them, became an attempt to describe one end of a continuum rather than a binary state. “Professional” is thus seen as purely adjectival, in the same way that defining someone as “educated” must either indicate a general state or that an arbitrary razor has been applied which suits the context. This view is dangerously attractive; for those looking to conduct case studies to assign or deny the status itself, the issue of definition is fundamental. Interactionists looking to criticise the self-interested actions and unjustified status of the professions will not need to look for a point of acceptance on a continuum of professionalisation since they will gravitate towards the worst offenders (Evetts, 2013). It is perhaps convenient to avoid matters of definition where one's thesis is one of criticising power and domination; a definition which included more lowly trades such as physiotherapists into professional status would rather upset a declamation of the huge financial rewards of membership of the professional caste, particularly as Hall (1968) suggested there is increased vocational feeling in lower-paid professions. Abbot's interest was less judgemental, studying the interactions of the professions as they strive to maintain their status in existing spheres of knowledge and capture new domains as they open up (Abbott 1988; Macdonald 1995, p.33), thus definitional precision was simply less important than observing their creation.

As an important aside, a fundamental challenge was made by Ritzer (1973), who criticised focussing on the general rather than individual cases. He suggested that whereas a profession

could be placed on a continuum, the individual practitioner could themselves vary in professionalism, and indeed a “professional” could be *any* person discharging their duties in a competent and diligent manner; a polysemy which persists today and is often used in place of a definition in modern writing. Public acceptance of this alternative model undermines the claims of a professional to be, by virtue of their career alone, the possessor of any particular distinction. Professionalism can today be considered a question of moral and ethical choices in a particular organisational context rather than a binary state for which an occupation might qualify (Delattre and Ocler, 2013). It must be stressed though that this is *not novel*; in the fifteenth century the term meant all occupations and went on to mean work done sufficiently well to charge money (Freidson 1986, pp.22–23). Being “professional” has undergone so much change that it can now be seen simply as whatever it is perceived to be (Hanlon, 1998). Focus switched to the motivations of the agitators rather than the strict enumeration of qualifying criteria. Famously Hughes reported his “Damascene” conversion:

“in my own studies I passed from the false question ‘Is this occupation a profession’ to the more fundamental one ‘what are the circumstances in which people in an occupation attempt to turn it into a profession and themselves into professional people?’”
(Hughes, 1963 cited in Macdonald 1995, p.6).

To conclude therefore, this study should not attempt to simply *classify* but rather *describe*. The aspects which are relevant to such a description will now be reviewed.

2.3.3 Theories of Formation

Wilensky (1964) was something of a turning point between the trait writers and those criticising privilege born of a claim of altruism (Collins, 1990). In the 1960s the US workplace had shifted from predominantly mechanical labour to more post-industrial work where managers were not fully able to rule on technical matters, producing more hybrid roles and a less stratified workforce (Freidson, 1973). Not coincidentally, the “semi-professions” begin to be recognised here: those whose claim to specialised training and to service orientation is partial or incomplete (Goode, 1960).

Wilensky’s contribution was interesting in two ways. Firstly, he developed a highly positivist theory of staged professionalisation based on statistically-treated hypotheses, which although not unique – Abbott (1988, pp.15–16) reviews this and others in a general denouncement of such structured process-driven work – is the most widely-known. These proposed stages were (paraphrased):

- People begin full-time work in the relevant area, forming an occupation.

- A training school is established, eventually supervising university tuition.
- The practitioners combine to form a professional association, which starts to shun as incompetent those outsiders who claim equal status, whilst forming synergistic hierarchies with semi-professions who do not. This eventually leads to control over entry, which creates conflict between the “old guard” who learned their trade more as craft skills and newcomers who followed the course they proscribed. Competition with other disciplines begins. This stage pre-dated the establishment of a training school in the most established professions.
- The association begins political agitation for legal monopoly, licensing and certification.
- A formal code of ethics and a “way to behave” is defined and enforced.

(From Wilensky, 1964)

Whilst the paper itself and successor work by Neal and Morgan (2000) show many variations on this sequence, it remains a useful model for discussion. The potential for tension between new and old practitioners as training evolves from inferred to taught can be observed, for example.

Secondly, alongside mastering an area of abstract knowledge, Wilensky (1964) uses *service orientation* as a qualifying criterion as a theoretical basis for the identification of professions, but does not accept uncritically the claims of the professionals on the matter. That interactions between patient and doctor are more likely to prioritise the client’s interests than those with a used car salesman is largely accepted. He foreshadows however works such as Freidson (1970) in discussing self-interest in medicine and Abbott (1988) for competition amongst groups for control. It is indeed around the 1970s that research focus moved from UK to US schools (Freidson 1986, p.28) and authors in that more anti-establishment age (Larson 2013, p.xix) became highly critical of the motivations of professionalisation projects.

2.3.4 Power, Autonomy, Exclusion and Self Interest

Following the lead of the Chicago School of Sociology (Larson 1977, p.xii), during the 1960s the questions moved from functionalist accounts of what professions *are* and what role they play to *why* they form and why they are granted privilege (Macdonald 1995, p.6). Notions of altruistic professionals as a positive “naturally present” social concept gave way to a more cynical evaluation of motive and self-interest. Authors emphasised the pursuit of power and status rather than the proper administration of a domain of knowledge; this drive for monopoly and exclusion through autonomy being pursued in a professionalisation “project” (Freidson 1986, p.29).

“Indeed, I believe that expertise is more and more in danger of being used as a mask for

privilege and power rather than, as it claims, as a mode of advancing the public interest”
(Freidson 1970, p.337)

Two schools emerged. The first followed the work of Weber which saw professionalism as a form of social closure, excluding others from an area of work by arrangement with the state (Saks, 2012). This usefully challenged the assumptions of previous writers that professions were a necessary social fact fulfilling some pressing need, by challenging the basis on which control was exerted and examining whether the claims of these groups were valid. This phase saw professionalism as a tactic to self-protect; by restricting the entry into the profession, supply and demand could be manipulated in favour of the credentialed (Macdonald 1995, pp.27–29; Saks, 1983).

The “closure” emphasis of Larson and Freidson moves away from describing an education and socialisation process, towards criticising the claim that mastery of the knowledge so imparted gives the profession the right to self-governance and self-certification of competence (Macdonald 1995, pp.27–29). Knowledge was alleged to unfairly set the profession apart, reduce its accountability outside those with equivalent knowledge and produce an asymmetry of power in the professional–client relationship. The professional thus becomes the route to “what is best for” the client, without the client being allowed to choose their priorities since they are not *qualified* to hold such an opinion.

It is clearly necessary to at least note the interest of the professions in excluding some of the competitive forces which would otherwise have diluted their income or status. Some (see Freidson 1970, p.363) advanced that by restricting the supply of the labour market, the aim of a profession is to recruit a sufficient number of like-minded individuals of requisite quality and maintain a good living from the inflated wage. Macdonald (1995, p.196) notes that early accountancy had to train unsalaried and under a master who demanded a fee. For the larger firms at least, this ensured that the entrants into the profession were *gentlemen*, with an independent private income, thus ensuring the continued prestige of the firm. Such writings however did become rather political, for example:

“I do not believe that it is anyone’s prerogative ... to impose his notion of good on another. I believe that the greatest good is each man’s freedom to choose his own good”
(Freidson 1970, p.376)

Under particular pressure here was the claim to altruistic service, itself a foundation of being trusted to self-govern. Authors did not necessarily reject the necessity of organising vital occupations to ensure competence (see Freidson 1994, p.194); their criticism was that the *altruism* enshrined in the ideal type put forward as a justification for disproportionate reward

was not demonstrable (see particularly Saks, 1995 and Freidson, 1970). As claims of altruism supporting monopoly are not a theme in the security literature this is perhaps not a priority for research, however it is the claim to ethical and disinterested practice entirely to the benefit of the client (outside a fee) which underpins the rationale for the state granting monopoly of practice.

Ownership of knowledge then excludes others from meaningful debate and hence places the professions as powerful gatekeepers to needed services (Freidson, 1986; Johnson, 1972). Power however is a relative term; as Freidson admits, ultimately only the apparatus of government actually possesses true compulsive power and can override advice for political ends. See for example the debate (Dyer, 2008) on cannabis classification, which saw the UK Government politically overrule its own professional scientific advisors. Society speaks of doctors' "orders" but with no ill-effects from insubordination (Parsons, 1939). Ultimately the power balance between state, profession and client dictates the degree of autonomy, since powerful clients are more able to dictate what services will be received, within overall regulatory limits (Downie, 1990; Larson 1977, p.xii).

The element of security's power over the client is therefore a potential angle for study, however not to excess. Power discourse became overly cynical (Evetts, 2003); Freidson for example later admitted (1988, p.384) that his criticism of 1970s medicine related to the privileges of a dominant profession during its most powerful period and not the general case. Saks (1983; 2015, pp.13–14) is critical of the contemporary tendency towards invective rather than empirically-grounded critique, which is noted ahead of the methodological discussion later. Freidson (1970, p.80) cites pharmacy's inability to prescribe as a sign of domination by medicine; this seems to confuse diagnosis and treatment of biological disorder (medicine) with absorption, interaction and pharmacokinetics of drug substances (pharmacy). Larson (2013, p.xxx) and Freidson's (2001) later work is more generous as seeing professional control as more acceptable than control by institutional management, however Saks's criticism remains a convincing warning against an obsession with *power*.

Professions could potentially compete to form hierarchies *within* their sector of society (Liljegren, 2012) which will be revisited below. Professions are after all strongly associated with high status and remuneration (Millerson 1964, p.13) and tend to remain in an educated section of society (Susskind and Susskind 2015, p.11). For Marxists however, viewing society as comprising the proletariat under the oppression of the bourgeoisie, the central question was where professions could be located in the overall social order. As professions grew from the expansion of higher education, they were variously seen as collaborators with the bourgeoisie

due to possession of knowledge capital (in lieu of actual capital), an educated subset of the proletariat by virtue of being co-controlled by the bourgeoisie, or as above a new stratum in society altogether (Saks 1983, Macdonald 1995, pp.41–50). Perhaps the most prominent such argument was Ehrenreich and Ehrenreich's (1979) "Professional–Managerial Class" which sought to position the professional, scientist and other intellectual as an interlocutor between the two outer layers of the former Marxist class dichotomy. Routine work is to be undertaken by the dominated proletariat separately from that of the privileged thinking class; professions ensure that anything resembling the routine (work which could be performed by a lower class) is removed to a subordinate profession or to trainees, to maintain their distinctiveness (Saks, 1983; Abbot 1988, p.126).

In vital public areas, even though ideological market closure rhetoric (see Freidson 1970, p.187) now seems almost *reckless* with respect to pragmatic protection of people from themselves, public debate concerning vaccination shows that for many *freedom to distrust* is still important. For specialist areas such as security, a case for granting regulation may become even harder to establish since the public may not appreciate the impact of poor practice (Stahl, 2008). As for self-interest, this should not fatally weaken the case for regulation provided the impact of incompetence is sufficient (Saks, 1995; Evetts, 2003; Stahl, 2006). Still, any progress towards self-regulation must therefore succeed against a presumption against monopoly born from this more critical phase.

It has therefore been discussed what professions are, what signs to look for during their professionalisation and why they face resistance to being granted monopoly. The section now goes on to observe how new professions jostle for jurisdiction over areas of knowledge.

2.3.5 The System of the Professions: Dynamic Formation and Competition

Professions claim *exclusive competence* over areas of knowledge and practice, however this is highly dynamic (Abbott 1988, pp.93–97). Whilst many never achieve this, the *ultimate* act of closure for a profession is to establish a legally mandated monopoly over their area of work, which must thus be granted by the state (Macdonald 1995, p.66; Freidson 1994, p.173) in its role as arbiter and legislator. Wherever there is a market niche however it is natural that there will be pressure on any monopoly. Defining the domain itself is not trivial; the applicant society must be able to show unity and competence in that domain, in addition to some great public *need* which is answered by granting this exclusive licence (Macdonald 1995, p.199) outweighing the corrupting concerns outlined above.

The contribution of Abbott's *The System of Professions* (1988), building on earlier work, was to

move conceptually from a model of stable professions which had achieved final closure in their fields, to a dynamic and territorially competitive model where professions compete vigorously and continually to gain control over contested areas of knowledge (Wilensky, 1964; Goode, 1960; Millerson, 1964; Muzio *et al.*, 2013). Where human advance and greater learning opens new areas of knowledge (Larson 1977, p.179; Millerson 1964, pp.79–84), the challenge to the existing professions is to *defend* their existing territory, or enter an agreement with an allied occupation. Alternatively, if the volume of work begins to routinise and dilute the skills required to perform its major operations, the elite profession can delegate to a subordinate semi-profession (Liljegren, 2012) as medicine has done with pharmacy, nursing and physiotherapy (Freidson 1970, p.47). A study by Davis (2011) of nursing competing for jurisdiction in the care of diabetes patients shows the potential of this model for examining professional identity.

Where control is only weakly established, competition can comprise direct challenges between professions, however this is impractical where legal regulation or monopoly has been achieved (Abbott 1988, p.95). More relevant to this study is expansion through technological evolution causing novel domains to appear, allowing the existing professions to fill the void of occupational control through competition, for example by expanding their certifications to include the new discipline and thus making a claim of ownership, illustrated in Fig. 2.



Fig. 2: A simple example of competition between existing professions relating to this study (examples given are purely for argument), based on the Abbot (1988) model.

In this modality, specialist sub-groups begin to form within the established professions. Although these professions may themselves lobby for control, if they fail (for example their resources are committed elsewhere or the claim leaves the body of knowledge incoherent) those specialists may consider it in their interests to collaborate. Should they no longer feel well-represented by the existing bodies, their internal networks can splinter to create a new professional group (Fig. 3). This can even be acrimonious, since the new group makes an indirect accusation of incompetence by distancing itself from the old (Goode, 1960).

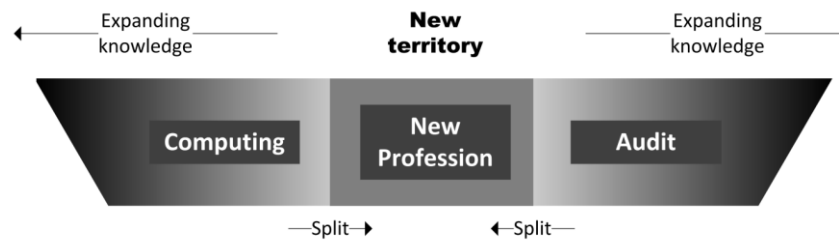


Fig. 3: A hypothetical example of Abbott splinter-based formation of a new group from amongst existing professions.

Whilst Abbott's approach is not without criticism (see Macdonald 1995, pp.14–17), it acts as a useful model, informing both data capture and analysis. Furthermore, it sensitises the researcher to concepts of fracture, competition, distancing from perceived subordinate groups, hierarchy amongst sub-professions, dissatisfaction with existing professions and the growth of new areas of practice. With its overlapping specialities and bodies one can see this movement alive in today's practice. Similarly, as security moves away from purely technical operations, the domain of physical security (itself multi-disciplinary) could make a move towards Information Security (see Griffiths *et al.*, 2010). Conversely since much recent movement comes from standards and regulation (Sundt, 2006), Information Security may border the knowledge domains of law and audit.

These areas of practice have developed certification bodies, with some supporting graduate qualification. The review moves on now to education and qualification, which are fundamental to a professionalisation project.

2.3.6 Education, Certification and Monopoly

Professions claim jurisdiction over a deep, discrete area of knowledge (Abbott 1988, pp.59–85). Universities have thus been fundamental to the transformation of the professions, both for their students and the professional academics who staff them (Freidson 1986, pp.15–59). As the acquisition of knowledge became central to control, training by apprenticeship gave way to formal prior education at university, exposing novices to cognitive standardisation. Larson (1977, pp.36–45) sees this as a vital step in the formation of professional unity with a shared and common understanding and orientation. It homogenises the professional association, therefore establishment of a monopoly over training is key to stability. Eventually, she argues, it becomes difficult to criticise eminent practitioners without criticising the structures of legitimation which attest to their qualification and knowledge. Similarly, once a project is sufficiently progressed for an orthodoxy to be established through control of a body of

knowledge, non-qualified practitioners can be criticised for their *charlatanism and quackery* (Johnson 1972, p.57) which is eventually used to justify monopoly.

Medicine is the “first amongst equals” of the professions (Crook, 2008) therefore one might expect medical education to be the seminal case. Physicians have long been required to be certified by a Royal College, however fellowship was originally restricted to graduates of the universities. This was absolutely *not* however because this guaranteed vocation learning: the insistence on graduate entry was to maintain the dignity and social status of the profession; early medical degrees had little to no medical content, there being very little scientific medical knowledge to learn (Reader 1966, pp.16–20; Larson 1977, p.4; Collins, 1990).

Education outside work is expensive, thus credentialed professions must achieve a monopoly on practice (or at least a sufficient premium) to have the prospect of recouping that investment (Larson 1977, p.15) and universities must ensure that their product is relevant to the job market. Professionals are socialised and educated at university and go on to learn the practical vocational aspects during the pre-qualification work period. Universities teach theory rather than train, such that the knowledge imparted is timeless and theoretical. There exists therefore an interplay between academic practice and professional practice, with the possibility of the academics and practitioners sharing a discipline but not fully each other’s working contexts (Becher, 1990).

An early step in the formation of a profession is the institutionalisation of control of entry, ethical conduct, discipline and quality (Lunt, 2008), of which credentials are a crucial stage. The formation of a central, controlling body to maintain standards condenses a group of like individuals into a coherent actor to which the state may corporately delegate jurisdiction (Freidson 1994, p.173) and which legitimates the claim to status through recognisable professional symbols (Greenwood *et al.*, 2002). Whether this represents the coordinated will of those individuals or the translation of the concerns of another actor will be explored later in the discussion of Actor–Network Theory. It is however well-established amongst the major writers (Freidson 1986, p.58; Larson 1977, p.5; 2013, p.xxiv) that it is the presence of a well-motivated and effective *campaign* by such a body which is significant in terms of progress, more so even than the quality of the claim itself. Larson (1977, pp.25–31) argues for example that engineering should have no inherent disadvantage compared to medicine in terms of status, but that the organisation of and claim by the latter was more effective, in part because the layperson has a more direct sense of success for a tangible engineered product (see also Freidson 1970, p.22).

According to many professionalisation models (for example Wilensky (1964) and for the first qualification by apothecaries in Reader (1966, p.52)), once specialists emerge and desire

certification of their specialist skills, influence is obtained first by the establishment of an association, then ultimately by this body establishing a monopoly over an area of knowledge, ideally granted by the state (Wilensky, 1964; Macdonald 1995, p.66; Freidson 1994, p.173). Unlike mainland European models (Neal and Morgan, 2000; Collins, 1990) which prefer top-down regulatory action by the authorities, Anglo-American governments have been wary of granting this delegation of power; candidates must first show that there is some greater public need which is thus answered (Macdonald 1995, p.199; Millerson 1964, p.216), and then that a profession has “the especially reliable knowledge by which to make decisions in the lay interest” (Freidson 1988, p.338). It is thus no surprise to see concerns about handing power to a professional body being raised in the current American debate (see NRC, 2013).

Professions must organise themselves into distinct roles, and delegate routine tasks to semi-professions or between the profession’s elite and its junior ranks (see the discussion of medicine in Larson 1977, pp.38–43). Nursing for example grew from craft to science-led profession, but its progress was hampered by failure to agree internal strata or create a professional identity (Elzinga, 1990). State control is often extended to the use of a *title* identity, linked to trusted roles such as “doctor” (Freidson 1986, p.65). A consideration of known and accepted *roles* in Information Security is therefore essential, as is whether a hierarchy of specialities is known and accepted.

Ultimately the professional is selling their learned wisdom; they are the “gatekeepers of desirable services or goods” (Freidson 1986, p.166) and *credentialed* professionals achieve that gateway status through exclusion. In the absence of regulation, credentials may gain *de facto* qualification status or count towards an unofficial tally of professional “points” (Freidson 1986, pp.63–81), but the ultimate goal of professionalisation is to control the production of the producers. The professional body must own the education and formation process in order to establish the necessary knowledge-superiority of professional over client (Larson 1977, pp.48–50). Credentials are required as markers for those seeking competent specialist advice (Freidson 1994, p.159; Collins, 1990). Their knowledge must have an apparently scientific and unified basis so that the knowledge foundation of the profession appears to be objective and dissociated with the preferences or opinions of the practitioner; the credential legitimates the professional’s opinion by being rooted in the entire profession and not the fallible word of the individual (Larson 1977, p.41; Wilensky, 1964). A binary status of *qualified* or *not* supported by a body of peers supports a claim to self-governance (Johnson 1972, p.55) particularly where this claim is based on the blessing of the neutral state (Larson 1977, p.70). What then if others suppress that independence?

2.3.7 Deprofessionalisation

Professions have the privilege of self-regulation (Larson 1977, p.x). Professionals generally accept technical control only by superordinate members of their profession, outside lay matters such as institutional targets and resources (Freidson 1986, pp.154–166). Much of the work in the field however concentrates on the suggestion that the professions have *declined* in influence (power) and independence as they have traded autonomy in sole practice for positions in bureaucratic organisations (Evetts, 2003; Clark, 2005). This external socialising force on internal workers leads to *conflicting loyalties* to employer and profession (DiMaggio and Powell, 1983).

Kahn *et al.* (1964) describe role conflict as “the simultaneous occurrence of two or more sets of pressures, such that compliance with one would make compliance with the other more difficult”. In itself Liu *et al.* (2001) found this to be a highly destructive event, associated with low job satisfaction and high propensity to leave, however they also found that a strong commitment to the profession moderated this effect as the professional would ally themselves principally with the profession and avoid the conflict. Moreover, aside from mere conflict Evetts (2003) argues that the modern professional is being entranced by romantic notions of status and dignity into being *controlled* by a species of imposed professionalisation (with its attendant high output, best practice and dedication to duty). This is even more relevant to this present study when one considers the necessity of *intention towards seeking status* on a professionalisation campaign (Millerson 1964, p.49; 1964, p.187), thus examining this intent is key.

“Deprofessionalisation” must be seen in context; professionals have always been *employed* even when in sole practice or retained by a patron, and thus have never had *absolute* control of their work (Freidson 1986, pp.110–123). Furthermore Kitchener (2000) found that when senior medics took up posts as clinical directors and gained financial responsibility, whilst they did adapt to bureaucratic priorities, the case for *deprofessionalisation* as hypothesised was less clear. Freidson’s “Third Logic” thesis (2001) positions ideal professional work between the extremes of bureaucratic control and market whim, as an example of a useful way to organise knowledge-based bespoke work. This is echoed by Fournier (1999) who sees the professionalised ethic and work-identity (with its emphasis on self-development and high levels of competence) as a positive model for controlling complex work within modern organisations.

Much modern writing therefore disputes the centrality of independence and emphasises the opportunities for the modern profession to control an area of work within large organisations (Muzio *et al.*, 2013) and the hybrid nature of manager–professionals (Noordegraaf, 2007). It is to this more modern world that the chapter now turns.

2.3.8 Professions in Modern Society

Development of the sociological theory of the professions has calmed following its “golden age” described above, despite the expansion of the professions and increasing emphasis on professional development (Gorman and Sandefur, 2011). Some interesting theoretical work has been forthcoming however. Sciulli (2007) for example challenged the understanding of the professions as an predominantly Anglo–American concept dating from the late nineteenth century by identifying a continental proto-profession which far pre-dates our received original cases. Brante (2011) revisited definition by proposing professions as “occupations conducting interventions derived from scientific knowledge of mechanisms, structures, and contexts”. This perhaps fits our more techno-centric society, but does not allow for the subjective nature of recognition.

As precedent, more relevant to this study are the numerous case studies of emerging professions and their identity formation; despite the decreasing prominence of the “self-serving monopoly” concept, interest remains high in the formation of new professions and the process by which this occurs (Adams, 2014). Gilmore and Williams (2007) as an example, took a pragmatic approach to definition in their analysis of the professionalisation efforts of Human Resources practitioners. Konstantinou (2015) examined Project Management as a profession with emphasis on whether the abstract nature of the archetypal professional knowledge base could be found in that discipline. There is perhaps no value to a complete survey of these studies, however their far higher emphasis on empirical work relative to the major works of sociological theory is noted. In such studies and following Ritzer (1973), a distinction can be drawn between:

- studies rooted in the traditional sense of *concerted social action* using the existing sociological texts as a lens for describing emerging cases, such as Swedish medical autonomy (Levay and Waks, 2009) or UK Matrons (Currie *et al.*, 2009), or the interesting suggestion that Information Technology is not professionalised (Mok, 2010), and
- the more modern status-neutral meaning of *most ethical best practice* which van de Kamp *et al.* (2004) preferred even whilst distilling concepts of medical professional behaviour. This reflects a particularly strong trend in medical papers noted during searches for this study which associate “professional” with “properly performed work” in that discipline.

Social and power concerns remain extant threads, however this stream now generally discusses

inclusiveness *within* professions across possible lines of (illegitimate) discrimination, alongside the declining power and increasing external regulation of modern professions (Adams, 2014). Whilst the development of *professions* by name has arguably waned, professionalism-related issues such as knowledge and power, status, inequality of reward and normative influences persist but subsumed into the sociology of organisations and management (Gorman and Sandefur, 2011).

Branching out from the traditional Anglo–American bias, more emphasis is being placed on work in a globalised workplace and other cultural professionalism models, for example in emerging markets (Brock, 2016). Similarly Saks (2015) contrasted Russian, British and American models of the medical profession to explore how the state’s interest and degree of engagement affects the independence of the profession from it. Taking this further, internationalisation of the business context and the existence of supranational regulators (such as the WTO and EU) has affected the interplay of actors which the older texts could assume to be national. Faulconbridge and Muzio (2012) survey the effects of these changes on and from the globalised professional service firms, particularly with regards to the differing nation-specific relationships with the state and degrees of autonomy of national bodies. Suddaby *et al.* (2007) similarly explore the regulation of professions with international reach, arguing that the traditional bargain of power in exchange for good governance between the profession and the state is being replaced by the global professional service firms and transnational trade organisations. Whilst the professional service firms’ market in international security practice is not as advanced as for the legal and accounting professions, this is an angle to be considered in a modern case study.

A more radical recent thesis however is that of Susskind and Susskind (2015), who see the growth of technology as fatal to the future claims of knowledge-based professionals. Extrapolating from the rapid advances in recent computing history and projecting towards intelligent search systems, they argue an expensive professional as a gateway to specialised knowledge will become an anachronism. They see no fundamental difference of type between currently retrievable information and that controlled by experts.

Their thesis is only partly convincing. Insofar as professional work is divisible into routine tasks and applied judgement, it is clear that the routine can always be more automated as technology allows; what is today a matter of judgement might in future be made more reliable by intelligent algorithms. Professional work however, particularly in organisations, is not exclusively based on clients asking factual questions for which there is a single right answer. Firstly, how does tomorrow’s body of evidence and knowledge continue to develop? It appears rather an

asymmetric analysis to imagine that everything other than technology remains static and predictable. Until legal systems are formalised it is difficult to imagine the lawyer; before computing the graphic designer; before YouTube's invention in 2005 the video blogger, yet all exist today. As the authors point out (Susskind and Susskind, p.290) there is a latent demand for professional tasks; more people need advice than can afford it. Surely therefore the greater ability of technology to perform tasks which can be routinised means that the professionals of the future will be engaged either in developing that technology or building upon its distributive potential rather than necessarily replaced by it.

Since little of today's use of technology could have been predicted ahead of its creation, it seems unlikely that one could predict how the availability of better tools will affect tomorrow's work. Since much professional work applies to human concerns and human life involves subjectivity, whereas a robot doctor could select treatments based on outcomes data, could it make a judgement about whether quality of life gains justify risk or discomfort? Could it counsel a divorcing couple, or predict the reaction of a judge to an individual's plea for mitigation based on contrition? Will the pace of technology change itself, as predicted by Larson (1977, p.27) render the routinisation of knowledge work permanently impossible? It is not possible to answer this today, however it is clear that professionalisation remains a relevant topic to research.

2.4 The Information Security Profession

Section 2.2 showed that Information Security has developed and grown in both scope, depth and importance to join the ranks of discrete occupations. In particular the emphasis on judgement, governance, risk management and cultural factors highlights the range of specialities vying for inclusion in this new candidate profession. Stepping back, section 2.3 considered precisely what a profession might be, and found it to be *imprecise*; more subjective acceptance than objective compliance with criteria. The section moves now to the confluence of these literatures and the subject of this study: the *Information Security profession*, its certification structures, roles and identities, ambitions and successes. To begin however it must be established why such a study is relevant and interesting today.

2.4.1 Why Study the Professionalisation of the Information Security Occupation?

The motivation for this work is two-fold. Firstly, from an academic perspective the professionalisation of Information Security is sparsely covered in the literature relative to the importance of its subject matter. Whilst there is much written by governments on the importance of training practitioners and by the associations attempting to support this growth, very little

independent scholarly scrutiny has been applied to either. Moreover, much of the work published is statistical and demographics data based on large-scale questionnaires and surveys, leaving opportunities for further work to explore their conclusions further. From a theoretical perspective, for example, how has a nascent profession – employed to protect intellectual property (likely to be held by corporations and governments) – fared relative to the more established professions which developed in smaller practices and which are potentially facing “deprofessionalisation” in bureaucratic organisations? How aligned are these new professionals with their peers? When people express views on certifications, what is behind that view and upon what is it based?

Secondly, although a professionalisation process can be conducted for benign reasons, many writers have warned of allowing monopoly and self-regulation. For some, to professionalise is necessarily to monopolise; without proper scrutiny and exposure to external judgement the profession moves from being concerned with what clients *want* to what they are “allowed to have” (Freidson 1970, p.350). For Larson (1977, p.xiii) autonomy allows the profession to choose which factors they will deign to consider, excluding the laity from their decisions and priorities. Similarly, Illich (1977) sees professions as self-interestedly defining what needs to be a professionally-treated problem in order to require more and more professionals (“They not only recommend what is good, they ordain what is right”). Security practitioners who establish power within their employer’s bureaucracies are in a position to act with a negative effect: security policies *control people*; control is of course sometimes required, however it is entirely legitimate to examine that control and criticise it where necessary (Stahl *et al.*, 2014).

Calls to license the profession require deep examination, to ensure that the motives, model and transition arrangements are fully considered (Pemble, 2001). If it does ultimately pass through regulation into monopoly, there is a substantial difference, as Freidson (1970, p.356) noted, between regulating people who charge money for their services, and requiring others to purchase those services. But exactly what services would one license? What is an “Information Security practitioner”?

2.4.2 Roles in Information Security

The identity of an individual exercising a *role* comprises organisational, social and personal elements (Ashenden, 2008). Having proposed that security now includes both technical and semi-technical management components, issues complicating a clear *single* profession include the lack of an identified and distinct *role identity* (Everett, 2011) and career structure (Hoffman *et al.*, 2012). The character of the Information Security practitioner is changing rapidly; whilst currently technical implementation skills are in short supply (DBIS, 2014a) there is a severe

projected shortfall of security staff with interpersonal communications skills (Frost & Sullivan and (ISC)², 2015a). The slowly-changing gender demographics in the occupation have been suggested as a possible source of more balanced skills (Frost & Sullivan and (ISC)², 2015b).

Where are the boundaries of the occupation? Much security policy is actually *executed* by network administrators (Adnan *et. al*, 2015); are these Information Security professionals? It might be possible to distinguish between technicians (firewall operators, network engineers, programmers) from the potentially professional security practitioner. The former are highly skilled tasks requiring detailed knowledge of specific aspects of technology, concerned with detecting and defending against attack with real-time systems, with an emphasis on staying abreast of current threats and techniques for using the various tools available (Kandogan and Haber, 2005). The professional security practitioner must be able to understand such technical risks and the responses available, but also assess the risk and produce business-led judgements.

As noted above, the security practitioner's role, title and even existence vary widely according to the security governance model in use at their employing organisation (Neal, 2008), as the new occupation struggles to define itself (Bowen-Schrire *et al.*, 2004). Named roles in the military hierarchy are well-established; the "Turquoise Book" for example (NCSC, 1992) lists the responsibilities of a US Government installation's Information Systems Security Officer (ISSO), however this is a hierarchical position rather than a professional identity. Similarly Ezingard and Bowen-Schrire (2007) found that in many organisations the primary functions of the "CISO" were in fact undertaken by IT managers, and that even where nominated individuals *exist* their job titles are "Risk Management Officer" and "Chief Security Officer". Whilst such titles may bring a cachet to the *role*, what does the putative profession advance as its own name? Any medical practitioner, in addition to their speciality, will identify as a *doctor*. A Chief Financial Officer could well be an *accountant* by profession, CFO itself like CISO is a rank. The roles of managers and board members with regards to security have changed since the topic became more prominent, however this distribution of responsibilities has received relatively little attention in the academic literature (McFazdean *et al.*, 2007).

Within the profession, it is also not clear what the progression and hierarchy of roles should be. Colley (2008) argues that the technical and managerial aspects of the profession are linked and that too much emphasis on the separation risks losing career continuity. This argument advances a directionality which implies progression from a technical role to a managerial one, accepting that technical knowledge may drop slightly upon entering a management role. This is not fully convincing; it does not address for example how the *different skill sets* of a technical and political role can be squared, since it is not clear that effective human-centric communication

and negotiation skills flow naturally from a technical role. As presented later, this progression was strongly contested in this study's data.

This identity incoherence was a founding concern for the Institute of Information Security Professionals (IISP) (Lacey, 2006) which codified a suite of roles in their *Skills Framework*, which has been taken up by government as the basis for their own certification scheme. Meanwhile "The Tech Partnership" (an association of employers, academics and like parties) maintains a comprehensive list of National Occupational Standards (Tech Partnership, 2016) which are then linked to the learning and certification schemes across the range of examinations above. Outside the UK, the National Initiative for Cybersecurity Careers and Studies (NICCS) has developed a similarly extensive "National Cybersecurity Workforce Framework" which lists a large number of roles with descriptions of key skills and example job descriptions.

Others will examine these roles in detail but the former chapter prompts the question: are these lived? Are they recognised and accepted in the profession and outside? And how are they identified? Whilst stratification is important for structure, for the profession to achieve formal state recognition there must be a clear boundary and criterion of competence; the state has an interest only in creating a list of the qualified (Carr-Saunders and Wilson 1933, pp.304–307); it is not interested in hierarchies and grades of membership.

2.4.3 The Certification Market and Professional Associations

Credentials are hugely important to practice; 87% of polled UK employers indicated that they would look for the CISSP when recruiting staff (DBIS 2014b). Today's IT practitioner in search of qualifications does not lack choice, both in provider (for example amongst many others IISP, (ISC)², BCS, City and Guilds, CREST and ISACA³) and grades of membership and examination. Some such as CREST cover a narrow band of practice, others such as the CISSP are more broad. Many have strong emphases on ethical behaviour, continuing professional development and professional practice skills. It is not proposed to review the entire credentials market; it is important simply to note its existence, properties, intent and range and move on to why they are offered and by whom.

The evolution of Information Security into a domain with constituent non-technical aspects has occurred very rapidly; so much so that many workers have predominantly had to acquire the new "soft" skills mid-career, rather than during their initial education and socialisation process,

³Full names given on page ix, however many of these no longer use their expanded form.

as would be the case for the more established professions (Siponen, 2000; Ashenden, 2008; NRC, 2013; Stewart and Lacey, 2012; E-Skills UK, 2013; Lacey, 2006). Although key aspects of their role, current practitioners lack confidence in their command of these new competencies (Ashenden and Sasse, 2013). This leaves a particular challenge for how to attain and establish competence for the modern professional, which is mainly achieved – fully in line with the sociological analyses of formation seen above – through certification by a professional body.

Without a common body of knowledge enforced by the profession, there cannot be a unified professional identity (Everett, 2011; Burley *et al.*, 2014; Orlikowski and Baroudi, 1988). The definition and delineation of a formal body of knowledge which can be assessed through certification is a fundamental part of claiming professional status (Griffiths *et al.*, 2010). Indeed professional identity is clearly the aim of many certifications, requiring both examinations and qualifying periods of experience. Since tests of knowledge should not require a mandatory preparatory period, these credentials are clearly meant to be the foundation to a professional claim of *experience, skill and judgement*, not simply the recall of learned facts. Whilst DBIS (2014a; 2014b) has investigated this from industry and academia to frame its next steps, this work was based on questionnaires and did not support a deeper analysis to discuss the point further.

The substantial range of certification schemes for security professionals available in the UK (issued by both international and national bodies) is not currently regulated by a single, national governing body authorised and delegated by government. When challenged to rationalise them during its own research, government refused to disrupt what it saw as a purely commercial marketplace (DBIS, 2014b). Knowles *et al.* (2016) however found that penetration testers saw visible CESG and CREST involvement as crucial to the standardisation of that part of the industry. Whilst it was seen above that this reticence to interfere in a profession unless necessary is common, it has hindered professional recognition since there is no clear single certification to recognise as a standard (Furnell, 2004; Tate *et al.*, 2008; Schultz, 2005; Everett, 2009) partially because of the wide variation in rigour and study time (Mansfield-Devine, 2013).

If these certifications can appeal to a sufficiently distinguished market based on some differentiated branding or emphasis then the *status quo* may be maintained, otherwise it may tip in favour of one particular qualification (Katz and Shapiro, 1994) making that organisation a *de facto* controller of entry to practice. This effect has been studied with interest in relation to IT standards, since the relatively swift rate of development and the degree to which standards interoperate and feed back within different sub-disciplines makes network effects particularly noticeable (Heinrich, 2013).

Why does this matter? A central organisation plays a critical role in advancing professionalisation; it distils member opinion, directs and represents their ambition, centralises their campaign, provides resources for development and facilitates networking (Millerson, 1964). By forming a society of practitioners apparently adhering to certain principles and of certified levels of competence, the institution provides legitimacy (Bloland, 1997). To that end, Lacey (2006) sets out the agenda for the IISP, founded in the UK in 2005:

“A new profession is struggling to emerge, in an ad hoc and piecemeal fashion, with little formality and structure. The contemporary scene is one of largely self-trained industry leaders supported by an up-and-coming group of ambitious individuals ... There is a need for a greater emphasis on professional development to develop future generations of well-rounded, fully trained leaders who can demonstrate ... that they are competent and effective”

(Lacey, 2006)

Lacey also builds an argument for the increasing importance of security (citing the increasing threat and increasing regulation) and thus the importance of ensuring competent management through better regulation and more formalised training. The latter part, supported by a complaint that security practitioners are self-taught invaders from other IT disciplines, is most interesting seen through the work of Abbott (1988), reviewed above.

Furthermore, the UK has a computing charter body (the BCS) with an active security chapter, therefore it is interesting that the IISP has also formed in the spaces around computer security, audit and computer law. The BCS also maintains qualifications and would appear to have a claim for supremacy from its Royal charter:

“to establish and maintain appropriate standards of education and experience for persons engaged in the profession of Computing or entering upon courses of study in Computing and allied subjects”

(Privy Council, 2003[1984])

Lacey (2006) mentions the BCS in passing, principally as a peer along with a number of engineering associations, implying that they would be advisory and supportive to a new institute representing Information Security practitioners. That the IISP and BCS *both* run security certification schemes (and that the IISP's framework has apparently found favour with the government with regards to assessing education) however is arguably an example of Abbot-type splinter competition for control of a body of knowledge, albeit that the organisations greatly overlap and cooperate (Mansfield-Devine, 2013). Whilst an argument can be made that the domains of IT Security (which the BCS might fully own) and Information Security (the focus of the IISP) are separate, writers such as Abbott (1988) and Freidson (1970) show that professions such as law and medicine have extended their reaches to cover gaps *far* wider than this in search

of dominance over an area of practice.

Ultimately such bodies allow security professionals to participate in industry and collegiate events (Brocaglia, 2005) which is a vital step to establishing an identity. Institutions are not necessarily benign forces however, even if established with pure motives; those at the top can be very well rewarded which may skew the priorities and behaviour of the organisation if an effective democratising process is not present (Schultz, 2005).

Perhaps the most significant recent work on the Information Security profession was the study by the US National Research Council (NRC, 2013) and subsequent paper by its lead contributors (Burley *et al.*, 2014), published after the data for this study was collected. The NRC was tasked with determining criteria for whether government should professionalise the US industry. This study, whilst extensive, took a relatively basic, trait-based model of profession (see also the online white papers on the subject by NICCS (2012a; 2012b)) and was based on public testimony from a large number of institutions, expert witnesses and professionals. The poorly-defined scope of Information Security practice and myriad potential roles and inter-relationships led the report to conclude that the occupation was not mature enough to be regulated as a profession. Whatever roles have been defined for the industry had apparently not taken root in the US context by 2013.

Whilst governments have been slow to introduce mandatory qualifications in private practice, they have taken steps to regularise entry into their own security ranks. The US 8570.01-M "Information Assurance Workforce Improvement Program" mandates baseline technical and management skills of staff occupying Information Assurance roles in the US Department of Defense (US DoD, 2010). Personnel fulfilling these roles (which are defined in some detail) are required to acquire and maintain particular qualifications, which may only be waived in cases of "severe operational or personnel constraints", the certification level required being commensurate with the designated seniority or technical skill level of the role.

Similarly, as part of the UK Cyber Security Strategy, the UK Government intention is to increase the level of professionalism amongst national security workers (CESG 2012a, p.3; DBIS 2014a). The stated aim appears to be one of ensuring a level of competence to a set standard of knowledge and awareness, as defined by the IISP. A hierarchy of competence status levels is defined and a series of body of knowledge streams identified. There is a directly implied link between professionalisation and competence to respond to increased threat (CESG 2012b, p.7). The hierarchy is cumulative for technical knowledge but not for other skills, such that it is possible to manage a team without being able to perform every job within it, however an "expert" must possess also relevant basic and intermediate technical skills (CESG 2012b,

pp.25–26). A brief code of conduct is included (CESG 2012b, p.31).

2.4.4 Security Education

It is not clear that a mid-career certificate alone can ever grant the holder *professional status* in its greatest sense; a graduate qualification usually providing a far greater symbol of learning than a certification (Schultz, 2005; Horrocks, 2001). Education, as opposed to training, is concerned not simply with learning techniques but also the rationale behind and basis for the action (Horrocks, 2001). Professionalisation is predicated upon control of the entire educational curriculum (Larson 1977, p.72). Professionalism is the application of substantial and abstract learning to the specific concerns of a client (Sciulli, 2007), which usually implies vocational graduate education (Evetts, 2003; Larson 1977, p.242). Hentea *et al.* (2006) see a preparatory graduate education as an essential foundation to the more transitory technical knowledge learned later in the career. Indeed the US DoHS (2012) and UK DBIS (2014a) see the expansion of tertiary education as key parts of their plan for their respective national workforces (albeit as a mix of paths to practice (DBIS, 2014b)).

Development of a recognised curriculum for security professionals has long been the subject of concerted efforts to harmonise and raise standards (Wright, 1998; Hentea *et al.*, 2006; Furnell, 2004) using inputs from all relevant contributors in an integrated manner (Hoffman *et al.*, 2012), teaching practical skills alongside theory (Sharma and Sefchek, 2007). Fitcher *et al.* (2010) argued in a study of South African tertiary Information Security education that the growing importance of this topic and the breadth of the study domain was leading to an increase in study, mainly postgraduate. In addition to the technical aspects, the higher level courses refer to more human-oriented issues such as ethics, adversarial thinking, privacy and the creation of policy, something found to be lacking in other courses but essential for modern practice (Ahmad and Maynard, 2014; Schneider, 2013).

Originally in the US but now looking wider, the National Colloquium for Information Systems Security Education was formed in 1996 to formalise the development of suitable programmes as a partnership between academics, government and industry (CISSE, 2016; Frinke and Bishop, 2004). Similarly after discovering resistance from computer science departments to include security as part of the computer science curriculum, a consortium of UK Government, (ISC)² and academia has cooperated to introduce cybersecurity as a component in all UK computing science degrees under the watch of the BCS as accreditor (Irons *et al.*, 2016; (ISC)² and CPHC, 2015).

It is instructive in both cases that these are the result of cooperative action by consortia.

Whether any body other than the UK Government could have *forced* the changes to UK academia for example seems unlikely. In one sense the action shows progress by those bodies in their control of educating the next professionals, however it is also the action of a security body in the realm of computing via another body. This suggests an incomplete level of professionalisation according to the models reviewed previously, since although there is therefore evidence of organisation, security curricula are clearly *not* yet set by a regulatory body for the occupation. Notably, CESG⁴ (2014) chose the IISP Skills Framework as a basis for the assessment of postgraduate academic study. It has also intervened in the market for master's degrees and academic study (DCMS, 2016), is extending this to bachelor's degrees (CESG, 2016) and is encouraging students into the profession (Ensor, 2016) but it has used its own branding to promote the result rather than empowering the IISP or BCS. The latter action, after a campaign for recognition, would have been predicted by orthodox theoretical models of British professionalisation (Neal and Morgan, 2000).

Given the high value placed in the literature upon the socialisation process at university (teaching of "norms" to new inductees aligned with their professional identity rather than any later specific appointment) (Olmsted and Paget, 1969) it would be interesting to note how any increase in graduate training homogenises the identity of the profession.

2.4.5 The Role of Ethics

Security management has a strong ethical dimension, needing to balance protection of a person's livelihood with restricting their freedom and personal rights. It can both protect a person's privacy from some colleagues and compromise it for others. Moreover, systems introduced for one benign purpose can be later misused for another far less pleasant purpose (Neumann, 2004). It may even, in certain defence and military applications, carry a moral dimension where the individual's skill is being used deliberately to target others (Fairweather, 2004). This places an ethical responsibility on the professional, a common trait seen in the professionalism literature.

Gotterbarn (2004) reviews many codes proposed for regulating behaviour, which some will put forward as a foundation of ethical professional practice, whereas the more cynical later professionalism writers (e.g. Freidson (1994, p.174)) see them simply as symbols of persuasion for those desiring the trappings of professional privilege. If calls for an ethical code are cynically motivated, they are not outwardly so; Oz (1992) argues that the need for a unified professional code (which should guide the professional during employer–profession conflict) is

⁴ CESG is at the time of writing rebranding as the National Cyber Security Centre.

rooted purely in the obligation a consulting profession has to the public. Blakley *et al.* (2001) were strongly critical of risk management practice outside a framework of ethical commitment to follow an approved methodology, favouring a licence which could be withdrawn under circumstances of poor performance or unethical behaviour. The researcher must be ready to look for such codes, albeit understanding that the presence or absence of such a code does not signify professional, or non-professional status since its necessity depends heavily on the domain of practice (Millerson 1964, pp.6–9).

Having established a research tradition for the Information Security profession but also the existence of several relatively unexplored areas, the chapter concludes by identifying and summarising the specific focus of this study.

2.5 Summary and Statement of the Research Questions

It was seen that the field of Information Security became prominent as society became increasingly dependent on computer processing systems which were vulnerable to attack. Whilst the protection of earlier systems was mainly a concern for their technical operators, gradually the importance of socio-technical and pure behavioural aspects created a sufficiently wide body of knowledge to support the creation of a new occupation.

The boundaries and specialist roles of that occupation are the subject of ongoing efforts of definition. Whilst governments and professional bodies have created frameworks to describe and contain the whole continuum of the occupation's area of knowledge within one overall label, it is not clear how much unity and identity of that over-arching "security" role is shared between its practitioners, nor how well-accepted those specialisms have become. The necessity for the modern security function to attract senior management support for its policies and interventions in operational processes, to ensure awareness of security topics amongst colleagues and to win support and co-operation with policy implementation and compliance efforts, whilst at the same time ensuring the competent detection of technically-based attacks, defend against them and prosecute the attacker, creates heterogeneity of skills under a single banner. The work of Abbott and others showed that this can be fertile soil for disharmony and incoherency. Myriad training and certification schemes exist in this occupation's name, however. Degrees are offered, professional bodies exist and now governments are dictating its shape and form. This field of work therefore is ripe for study.

The title question *cannot* be answered simply and objectively; there is no metric which can be applied nor binary status to be awarded. One can only observe the occupation and frame an answer descriptively based on the theoretically-predicted journey of a professional project. The

opportunities to advance the field therefore start with that project's origins. It was seen above that professions are formed through fragmentation, amalgamation and competition between neighbouring disciplines. Juxtaposing this with the history of security suggests that some events within Computing created tension and eventually fracture to create a distinct occupation; whilst some academic and historical accounts exist for the practice, this question of the origin of the *profession* and its identity formation is not firmly settled. Furthermore, examination of this empirically amongst those in the industry itself is particularly suitable for research since it is relatively unexplored.

Once a new specialisation emerges, theory suggests that it will need to form a distinct identity with its own culture and customs, therefore this represents the second main thrust to an account of that project. The knowledge base of this occupation is well-described by several bodies precluding useful addition, however the real-world distinctiveness and separateness of the occupation from its parent are not. For example, aside from a panoply of rather mechanistic and unconvincingly positivistic accounts of how to cause obedient behaviour in human policy targets, there is little research into how human factors are incorporated into facets of the actual practice and training of this profession. How are these new skills learned? How do those practising them coexist with technical specialists? It can be seen from Neal (2008) and from numerous surveys that there are a variety of reporting lines and titles within businesses, but as Information Security has occasionally claimed to be greater than mere technical implementation of policy, *should* the CISO continue to report to the CIO (from their own perspective), and why?

The status of Information Security's professionalisation has been explored only at a high level, under a rather basic model of profession. What is the orientation of the occupation's own workforce with regards to professional status? The literature remarks on the actions of governments on the national stage and others have commented and will doubtless *continue* to comment on them. What is not clear however is to what extent these are supported by and representative of opinion within the industry, which is made relevant by the import placed on this by the professionalisation theory. Which of the concepts of "profession" actually find resonance within the occupation and how is this label received or desired by them? What is the extent and influence of credentialism, which the professionalisation literature regards as central to the success of a professional claim? Is licensing desired and would the government support it? These topics have not been explored fully and present an interesting opportunity for empirical study. Therefore, distilling and filtering these areas for research the following specific questions were proposed:

- What are the origins of the modern Information Security profession?
 - When and why did Information Security roles emerge and separate from Information Technology to form a new profession?
- What is the current status of the Information Security profession?
 - To what extent does a discrete area of practice exist with which the practitioners associate and what is its status?
- What are the prospects of further professionalisation?
 - Are there ongoing projects to professionalise the industry, what are their aims and are these being achieved?

Chapter 3: Theoretical Basis

In responding to the research questions it will be necessary to develop a research strategy and methodology, in preparation for which this chapter explores the socio-philosophical perspective from which the work is approached. The use of Actor–Network Theory within the work will be explained and a summary of the philosophical foundations of this approach presented.

3.1 Introduction and Glossary

Before social research can be undertaken one must select the philosophical approach to be taken, however variations in definition for philosophical terms create challenges. “Positivism” for example can be found used as representing an entire philosophical perspective or simply an epistemology (Hollis 1994, pp.41–42). In this section therefore the usage of these terms here is clarified below, drawing from the well-accepted conventions of Burrell and Morgan (1979).

Ontology	A theory as to the nature of reality, in other words: <i>what exists</i> . The principal point of discussion is whether there exists an objective social truth (knowledge about concrete social structures “exists” ready to collect, realism) or whether reality exists only for the individual as artificial concepts which are given shared names (nominalism) (Burrell and Morgan, 1979). Since it defines what can exist, ontology is the foundation for all later considerations (Holden and Lynch, 2004).
Epistemology	How knowledge can be obtained or experienced. It is necessarily coupled to ontology, since one cannot “know” what one does not accept exists. Can one “know” social reality by hypothesising, testing and measuring it (positivism) or is it individual and can only be understood by interpreting the positions of others? The latter position is occasionally referred to as “interpretive” epistemology, however this will cause confusion with interpretivism as a paradigm (see below) thus the Burrell and Morgan (1979) adoption of the general term anti-positivism is useful.
Voluntarism and Determinism (Agency)	Is a person constrained by their surroundings: are they an “actor” with free will to choose how to act (voluntarism), or an “agent” playing out their role in a social structure (determinism)? Hollis (1994, p.107) actually places this in ontological terms: one accepts individualism (the individual exists) or holism (social structures exist) whereas Burrell and Morgan (1979) place it

external to ontology. Between these extremes, Jones *et al.*, (2004) note that Giddens' Structuration Theory acknowledges both that the human is affected by structure (by learned and reproduced behaviours) but makes choices which – albeit potentially with consequences – they are free to have made differently.

Methodology and Method	“Methodology” will be used to describe the underlying logic of the research approach, whereas “method” will refer to the specific techniques. Nomothetic approaches look at the general behaviour of groups, considering the individual to be a member of that group and affected by common laws. These approaches are often linked to systematic measurement and testing of hypotheses, and hence are frequently linked to the positivist epistemology of natural science. Ideographic approaches focus on the individual, aiming to produce a full description of a particular case and recognising its uniqueness, without necessarily taking a highly regimented and reproducible empirical approach (Burrell and Morgan 1979, p.6; Gibbs 2007, pp.5–6).
---------------------------	--

A study will choose methods which produce the type of data which aligns with the chosen methodology. A nomothetic methodology will tend to desire the production of quantitative data, to demonstrate correlations between observable variables, observe trends or test hypotheses. It will therefore favour methods which produce population data minimising the role of the individual, such as the survey. Ideographic studies will conversely look to observe and collect the idiosyncrasies of the specific case, such as by interview (Burrell and Morgan 1979, pp.6–7).

Method selection is output-specific. To review the performance of a drug it is desirable to remove any bias or placebo effect from the results. Where understanding is less well developed and the question less distinct, numerical data cannot completely explain nuance in the meaning and intention of actions, for example what it means to contract the relevant illness (Flick, 2009).

Paradigm

Clearly ontology, epistemology and methodology are linked. Taking the nominalist ontology that there is no objective truth but then adopting a positivist epistemology, to measure and test reality objectively, creates an internally inconsistent position. Some authors have therefore identified *paradigms* which describe a reasonably coherent philosophical approach, analogues of political parties or schools of thought, grouped for convenience of reference (Burrell and Morgan 1979, pp.23–24). As these authors state (p.36), this is far looser than the Kuhnian paradigm which defines the exclusive mindset for a generation. They suggest that sociological positions can be classified on two independent dimensions, which together give four paradigms. The first dimension (“subjective–objective”, illustrated in Fig. 4) is an axis between a natural science approach to social questions (sociological positivism) and requiring understanding from within rather than describing from without (derived from German Idealism).

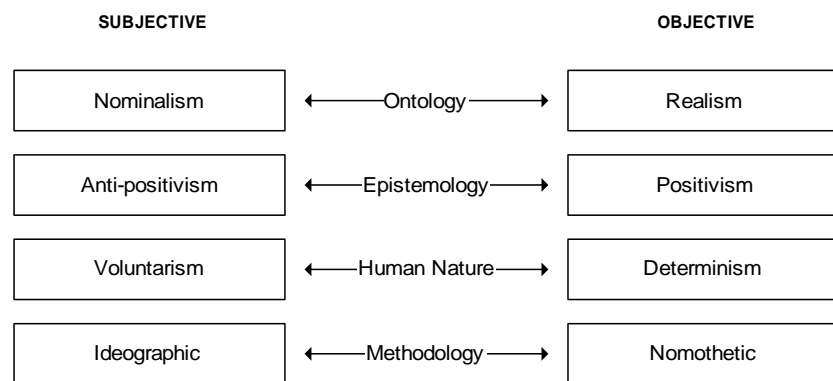


Fig. 4: Subjective–Objective dimension (Burrell and Morgan 1979, p.3).

The second dimension, shown in Table 1, considers order and conflict; work might account for the status quo with well-established and integrated elements, whereas other work will describe change, instability and coercion rather than consensus. Since well-ordered change can be part of the maintenance of the status quo, they draw the distinction between regulation (which can include integrated processes of evolution) and radical change (which is an agitation).

<i>Regulation</i>		<i>Radical Change</i>	
(a)	The status quo	(a)	Radical change
(b)	Social order	(b)	Structural conflict
(c)	Consensus	(c)	Modes of domination
(d)	Social integration and cohesion	(d)	Contradiction
(e)	Solidarity	(e)	Emancipation
(f)	Need satisfaction*	(f)	Deprivation
(g)	Actuality	(g)	Potentiality

Table 1: Regulation–Radical Change dimension

(Burrell and Morgan 1979, p.18)

** In other words, whether the system is geared towards the satisfaction of individual needs.*

The poles of these two dimensions produce four *paradigms*, shown in Fig. 5:

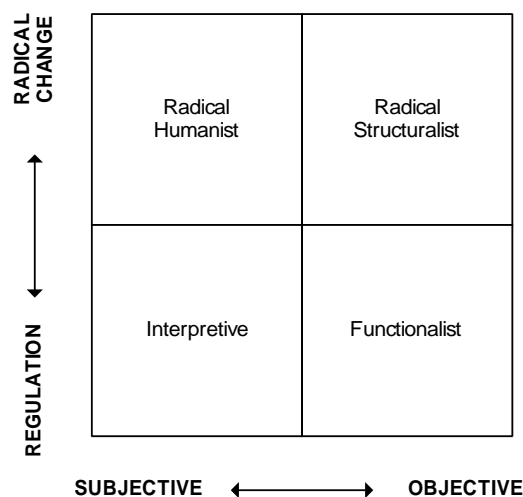


Fig. 5: A model of four sociological paradigms (from Burrell and Morgan 1979, p.22).

Chua (1986) rejects both such strict dichotomies and the separation of Radical Humanism and Radical Structuralism, preferring *mainstream* and *interpretative* positions (akin to functionalist and interpretative paradigms above) with the Critical tradition as the final perspective. Critical perspectives are distinguished by emancipation and ethical evaluation; interactions are viewed in terms of their restrictive effects on the individual, who cannot reach their full potential due to structures of domination (Chua, 1986).

3.2 Prior Trends

Having defined our terms, to position this as an evolution of the existing literature and thus support a claim to advancing it, it is useful to consider the prevailing theoretical traditions.

3.2.1 Dominance of Positivism in Social Studies

In its exploration of the physical world, natural science has adopted and honed the hypothetico-deductive model attributed to Newton (Bernard 2000, p.12; Chua, 1986; Galliers and Land, 2002). Implicitly this assumes objective truth, where objects will obey set laws regardless of the understanding of any observer. Hypotheses which are tested repeatedly and successfully become theories, which can then be used inductively to create other hypotheses, growing stepwise the body of known truth (Hollis 1994, pp.40–65). Eventually new techniques of testing and observing create results which disprove those theories which are fundamental to that paradigm and hence the paradigm itself must shift to encompass the new observations (Kuhn, 1970). Whether or not the study of natural phenomena is genuinely as divorced from the social reality of the human researcher as is claimed (see Latour, 1988), this model, variously described as positivist or functionalist, remains the dominant position in natural science research.

Positivism can also be applied to social studies however here it is more controversial. Although a considerable number of social scientists still favour such a “natural science” approach (Lee, 2002; Burrell and Morgan 1979, p.25) many philosophers of social science have moved away from a positivist position. Dilthey, for example, argued that there is a distinction between descriptions of inanimate objects – which cannot interpret the context in which they exist – and humans to whom the world exists as a web of meanings and from which they are inseparable (Barnard 2000, p.19). They must therefore be understood rather than explained, including such concepts as *value* which do not apply to the natural sciences (Hollis 1994, p.17).

Of particular note is the substantial amount of work examining user security behaviours and policy compliance. Such studies often take a positivist stance, through hypothesis-testing by survey. Demonstrating direct effects of awareness and policy, even if accepted epistemologically, is challenging in practice due to the difficulty of gathering data on real behaviour (Crossler *et al.*, 2013). Behavioural constructs such as General Deterrence Theory, Protection Motivation Theory and Value-Focused Approaches are invoked in these studies to explore why behaviours vary from those expected or desired. These studies are still of interest to the constructivist however, by describing a conceptual and motivational tension between context, policy author and subject. This study, following Siponen (2005), considers that whilst positivism is well-accepted in the study of computing science, the mechanistic “cause and

effect” studies of user behaviour and compliance might be viewed with some caution and empirical interpretative work has much to offer.

3.2.2 Research Traditions in Information Systems Studies

It is useful to adopt the distinction made by Stowell and Mingers (1997) between Computing Sciences (CS): a technical domain concerned with computer systems, and Information Systems (IS): the application of those systems where they are put to use. IS research arguably began in the 1960s within the study of the development and use of IT in a business context (Myers and Avison, 2002) however the precise boundary between the two areas is not universally accepted (Stowell and Mingers, 1997).

This is not surprising since it is reasonable to assume that the two are in dialogue; commercial computing systems (at least) would not be financially viable were they of no use, and the application of computing systems within IS is linked to the capabilities of current technology. There are clear parallels between the CS/IS distinction noted above and that made between the technical aspects of security (such as the design and analysis of the algorithms used for encryption) and the policy and governance aspects noted in the previous chapter. In the discussion of research trends below therefore, this will refer predominantly to IS research rather than computing.

Historically, like its natural science origins, IS has been associated primarily with a realist, positivist approach using quantitative data. (Orlikowski and Baroudi, 2002; Siponen, 2001; Myers and Avison, 2002; Galliers and Land, 2002; Siponen and Oinas-Kukkonen, 2007; Dhillon, 1997, pp.8–22). Dhillon and Backhouse (2001) describe this as aimed at producing “practical solutions for practical problems”, characterising the approach as in the Durkheim school, using natural science empirical methods upon a social order which possesses concrete artefacts.

By (2001), Dhillon and Backhouse saw movement in the IS literature towards a more holistic and socially-informed outlook, but this was not often apparent in the security subset of the literature. In this, they report a preponderance of checklists, procedural and mathematical risk analysis models and evaluation criteria which fail due to offering a “rational explanation of social affairs” whereas emancipatory (Critical) approaches still appeared scarce. Since security policies restrict personal freedoms and Critical theorists seek out areas where forms of domination prevent the fullest expression of human freedom (Chua, 1986), this is surprising, since Critical Theory should be highly suited to this line of investigation (Stahl *et al.*, 2008).

By contrast, much of the security *management* literature is conceptual, elucidating novel frameworks or perspectives. Whilst some is of high quality, the lack of empirical work, rigour and theory overall has been criticised (Siponen *et al.*, 2008; Cannoy *et al.*, 2006; Silic and Back, 2014; Willison and Siponen, 2007). Fulford and Doherty claimed as late as (2003) to present the first serious empirical work on security policy. This is strikingly similar to McGee's (2006) review of physical security literature which found little quality empirical academic material and much subjective opinion and proposals for frameworks.

There is a clear recent trend away from this dominance. Siponen and Oinas-Kukkonen's (2007) review of early 2000s literature reports the continued dominance of mathematical, procedural and technical approaches, stating the need for more theory-creating qualitative empirical work in the area of security management. McFadzean *et al.* in (2006) still reported a dominance of functionalist research in the traditional mould, but with a significant strand of human-centred holistic work emanating from security's shift from a technical to a socially-informed topic. More recently still, Myers (2011) reports more interpretive work, estimating that it constituted around a quarter of contemporary research, albeit that Critical research was still under-represented.

3.3 Selection of Theoretical Perspectives

It was shown above that whilst positivism has dominated early security work, Information Security studies are increasingly taking an interpretative approach due to the increasing recognition of human and governance factors. The review moves on therefore by positioning this study within that context by identifying its theoretical foundation.

3.3.1 Selection of a Socio-Philosophical Paradigm

There is some freedom here. This study, as an examination of the status of the profession rather than the technical work they supervise, is not bound to continue in the functionalist "tradition" since there is a substantial precedent for work in other, more interpretative, paradigms. Much of the previous work is not empirical (Silic and Back, 2014; Willison and Siponen, 2007); whilst empirical work is not necessarily superior (Stahl, 2014) this bias provides an opportunity for novel contribution to empirical work.

Critical theory, the third of Chua's (1986) "world views" (paradigms), would be a useful platform to explore the impact of a rise of a professionalism movement within security governance, especially with regard to the impact on privacy, freedom and workplace dignity which could potentially be curtailed in the name of security (Stahl *et al.*, 2014). It is particularly

suited to the exploration of a new breed of manager exercising control over employees using a lever which has considerable purchase with senior management, with considerations of liberation or emancipation (Klein and Huynh 2004, pp.167–168).

Although by no means the only benefit of the approach – much can be learned by management as well as the advancement of the managed (Stahl *et al.*, 2008) – this broader emphasis on emancipation is not aligned with the research questions identified; the nature of such a study would be to advance such a particular liberal cause. Whilst the exploration of such themes of dominance is highly valid for future work, there is no such agenda available to advance in this specific study.

Attention moves then to the more neutral functionalist–interpretative continuum. A fully functionalist approach is troublesome; the aim is to explore and explain the existence, status and aims of a professionalism movement, however the review of the professionalism literature concluded that an objective definition of professional status cannot be achieved as it is so highly subjective. Leaving aside an ontological discussion about the reality of such status, how could one adopt a positivist epistemology when there is nothing clearly defined to test and measure outside any given individual’s understanding?

So is an entirely interpretive approach suitable? There will be a core group of any occupation who consider themselves professional and wish to be perceived as such. It must be identified whether this is a significant or influential group matching a general intention in the group. This could be approached with a positivist epistemology using surveys, which would give a good claim to generalisability amongst the population, however as noted the subjectivity inherent in professional status discussions aligns well with an interpretive standpoint. Knowledge of reality is, in this approach, gained through social constructions (Klein and Myers, 1999).

An ontology whereby social reality is entirely constructed is also difficult. Abbotonian professionalism can be seen either as a movement from within or the opening of space by an external cause widening a field due to technological advance. Viewing a professional movement purely from a subjective viewpoint may hide the action of non-human events. The approach must be neutral on this point and not pre-judge the causes of such a movement.

3.3.2 Consideration and Selection of a Theoretical “Lens”

In addition to the selection of a philosophical basis for the project, it is possible to use a lens or sensitizing device as an additional theory component to aid interpretation. Gregor (2006) identifies various categories of theory, from those used to simply frame the analysis (such as

schema, taxonomies and frameworks) through to comprehensive prescriptions of method and technique. Between these lie theory used to explain or predict phenomena; these are more abstract and represent ways of viewing or explaining the world.

Such theories are typically philosophical and sociological in origin and require adaptation to ensure the technical aspects of IS-related study are included. Johnston (2001) proposes “we should not be borrowing theories fully-made from other disciplines but rather taking the essential features of these theories which are useful to IS studies”. Lee (2001) elaborates on these features:

“[IS] research ... examines more than just the technological system, or just the social system, or even the two side by side; in addition, it investigates the phenomena that emerge when the two interact... our field's so-called ‘reference disciplines’ are actually poor models for our own field. They focus on the behavioural or the technological, but not on the emergent sociotechnical phenomena that set our field apart.”

(Lee, 2001)

Within the group of theories for “understanding”, Gregor (2006) identifies high-level theories which are used to form a world view (such as Situated Action, Actor–Network and Structuration Theories) and low-level theories used to explain specific phenomena (field studies, surveys, ethnography, hermeneutics and phenomenology).

Hermeneutics is concerned with interpreting the meaning of text, from the point of view of a subject where the same event has different meanings for people with different life experiences. Myers (2004) suggests that its core principles of finding meaning in text (along with phenomenology) underlie the interpretivism concept. Alternatively it can guide the research process, understanding a controversy from the viewpoints of the conflicting observers, working until all apparent contradictions have been explained using all available information. A key concept is the hermeneutic circle: one’s understanding of the whole of a phenomenon is informed by studying its parts, however those parts are likewise understood in terms of the understanding of the whole. While useful in the IS context, it is most applicable to situations where a controversy needs to be understood within a particular context (Myers, 2004), whereas at design time it was not known whether the viewpoints of the various actors in IS Security necessarily conflict.

Phenomenology similarly includes elements of pure philosophy as well as a structure of application. Husserl’s transcendental approach attempts to disregard what is not truly fundamental to reduce the concept to its pure “essence”, achieved through deep analysis of the term’s meaning and even etymology (Introna and Ilharco, 2004). It was considered impractical to view security professionalism through such a lens since both security and especially

professionalism are notable for their manifest lack of a satisfactory definition. Such an analysis could find it difficult to identify the essence of what a generation of sociologists struggled even to define in broad terms.

For Jones *et al.* (2004) Giddens's highly influential theory of "structuration" intervenes in whether action is constrained by pre-existing structures or whether these structures emerge from action. He suggested that actors learn and reproduce certain patterns of social behaviour which become accepted in organisations or society, however these are not fixed properties and the person is not fully constrained by them. By electing to follow them according to a scheme of inducements and penalties, the actor reproduces the pattern for another instance. To Walsham (1997), Giddens's own work does not reference technology in much depth and does not provide substantial methodological support to those wishing to make use of it in IS studies. To address this and deepen the theory in this area, the "duality of structure" was referenced and developed by Orlikowski (1992) to apply these concepts to a mixed technology/organisation context, where technical features (which could include security policies, controls and enforcement methods) both shaped and were shaped by the patterns of usage. Later, Atkinson and Brooks (2003) combined the structural elements of Structuration with the symmetry of ANT to focus on and fully recognise the distinctiveness of the human-machine entity created by user-technology interaction, proposing "StructurANTion".

These approaches are potentially extremely useful ways to view a movement in security professionalism. This is particularly true in terms of the analysis of a case study of security technology within an organisation and its interaction with user behaviour (as developed further by Orlikowski and Robey (1991)). With its emphasis on identifying the work of a change-driving actor in human-technical networks (Brooks and Atkinson, 2004), Actor-Network Theory (ANT) however was seen to offer the most useful insights for the study of population movements strongly influenced by a technical context and the competition in a dynamic area to achieve social closure. It is particularly promising when combined with Abbott's theory of the "System of Professions" reviewed in the last chapter. The dynamic and competitive nature of the claims for jurisdiction in new areas and peripheral areas echoes the ANT concept of groups not being fixed entities but in existence only as long as the network stays stable (in this case that the profession continues to defend its domain against other networks and actors).

3.4 Actor-Network Theory

To explain the selection of ANT as a lens, it is necessary to offer a summary of its principal tenets.

3.4.1 Introduction

Actor–Network Theory – or the *sociology of translation* – grew out of the area of Science and Technology Studies in the late 1980s (Law, 1992), principally concerned with the study of scientific method by Bruno Latour, Michel Callon and John Law.

3.4.2 Sociological Roots: Knowledge and Facts

Law (1986, pp.1–17) traces the history of the sociology of knowledge in three phases. The first is seen as the work at the birth of the sociological discipline in the nineteenth century by Marx and Durkheim. Whilst both of these writers make a wider contribution, Law was interested in the dialectical relationship between social structure and knowledge. Marx, interested in the relations between classes and the continuation of that structure, was reported to see ideology as a mechanism for maintaining an (unequal) social order against the interests of those disadvantaged by it, thus that the individual can be encouraged to accept a social structure through a learned experience. Durkheim is cast in the debate between empiricism and rationalism, or rather as going beyond it to suggest that neither is completely satisfying in explaining behaviour; instead suggesting that:

“Our social classifications provide, so to speak, a template upon which we build our structures of thought. The social, as always for Durkheim, describes a reality that is prior to individuals.”

(Law 1986, p.5)

Whilst not noted in Law’s summary, Latour (2005, pp.13–16) also cites the work of Tarde as an influence, placing it in opposition to Durkheim’s views on society. In Tarde’s work, Latour sees the beginnings of the attack on an ill-defined “social” explanation for behaviour criticism of which later became a theme in ANT. This school (he says) would reverse the arrow of causality, turning society from an established and stable container for agents eternally “condemned” to be shaped by it, into microscopic actors whose independent actions create macroscopically observable effects which are labelled as social.

Law’s (1986) concept of the “first phase” ends with a hiatus in the 1950s as a number of intractable problems derailed the contemporary writers, following which the second wave emerges in the 1960s to re-examine those issues. This comprised a number of relatively independent threads based on the above two schools; of these, the most interesting in this context was also influenced by Douglas and the scientific history of Kuhn:

“Scientific knowledge was treated as a culture like any other form of knowledge, and was seen as being directed by social interests with the corresponding social control

implications.”

(Law 1986, p.2)

Law suggests that Actor–Network Theory emerged during a third wave in the 1980s. It proposed an approach which described the establishment of facts via networks of those who are persuaded to accept them rather than because of any inherent objective truth which they may possess:

“By itself a given sentence is neither a fact nor a fiction; it is made so by others, later on.”

(Latour 1987, p25)

Compare:

“As there is no neutral, objective world of facts which acts as the final arbitrator, the adequacy of a theory (or explanation of intention) is assessed via the extent to which the actors agree with the explanation of their intentions.”

(Chua, 1986)

Latour (1987) builds on this to criticise the foundations of modern natural science functionalism and positivism, questioning the view of science as an egalitarian pursuit of hidden natural truth, disseminating strictly vetted facts between peers. Latour offers an alternative mechanism, how the work of previous researchers is not in a binary and intrinsically held state of right or wrong, but rather accepted, enshrined and eventually invoked in a hierarchy of persuasion. Scientific writers attempt to convince the reader to accept their work as fact and recruit allies to his or her theory, not merely through writing but equipment, graphs, tables and any other medium. This theory grew to explain the provenance of established facts and how the network which accepts them develops and strengthens (Scott-Smith, 2013) opening the “black boxes” which represent those established facts (Latour, 1987) and how power relationships come to be embedded without assuming that a person is imbued natively with “power” as a property (Law, 1992).

ANT moved away from contemporary thinking by stressing the importance of the non-human actor (“actant” is sometimes used (Latour 2005, p.55) to avoid being drawn into a discussion of human agency). The early movement is fairly coherent and stresses agnosticism on the part of the observer of the physical nature of an actor and strict symmetry of treatment for human and non-human actors alike (Latour, 1987; 2005; Law, 1986; Callon, 1986). Later, however, the field so diverged that there is no longer a common body of knowledge, unity of application or standard for account structure (Cho *et al.*, 2008; Walsham, 1997; McLean and Hassard, 2004).

3.4.3 What is the “Social”?

The proponents of ANT emphasise that they are not proposing a novel research method but rather an ontology, or possibly even simply a challenge to the existing sociological mindset.

Certainly Latour's (1987, p.7) language of "abandon[ing] knowledge about knowledge" implies an epistemological and ontological position; Sayes (2014) positions it as primarily a research methodology however as Gad and Jensen (2010) note, little detailed method is provided by its main proponents other than to reject prior assumptions of macro effects.

It can indeed be difficult to define the project exactly as its proponents seem keener to detail what it is not. Callon (1999, p.194) for example states, "ANT is not a theory. It is this which gives it its strength and adaptability". Observers might then query "theory" in the title (Gad and Jensen, 2010) however Callon (1999) suggests this was applied from outside rather than a claim by its proponents. Latour has also addressed (1999a) the technical, predictable and inflexible associations which have become attached to "network" since the explosion of internetworking, and the controversy surrounding the "actor" as a source of intentional action. ANT might be thought of at the level of ontology or even paradigm rather than a specific and procedural method.

One of ANT's principal criticisms is of the existence of "social stuff", that there is a social mechanism routinely invoked for explanations of phenomena without justification (Latour, 2005). Law (1992) notes that one cannot, when trying to explain the existence of social structures, begin by assuming that they exist; to do so is akin to a teleological position that infers the presence of an ethereal "social force" from observing what are taken to be its effects. Similarly, Law claims that one cannot assume the rich and powerful to be constructed from essentially different social materials from the poor and lowly but must explain how this unequal situation arose and how one set acted in their environment to enlist the co-operation of others.

"...the social is nothing other than patterned networks of heterogeneous materials"
(Law, 1992)

3.5 Controversies: Sources of Uncertainty

Latour's seminal work "Reassembling the Social" (2005) lists five key areas (pp.27–139), which might be loosely classed as dimensions, where ANT departs from traditional thought, which are paraphrased below.

3.5.1 Groups

ANT suggests that groups are not static, fixed and settled items, but rather dynamic and in continual formation (Latour 2005, pp.27–42). There are no pre-existing innate groupings or classes which can be brought unexamined into an explanation of action. Rather there are associations of individuals, seen in the act of association and in the attempts to defend the group

integrity against externals (who may be attempting to recruit members to their own cause). Such movements leave traces which can be seen and thus included in the account. Once the association is no longer active it is no longer doing any work, and thus it has been disbanded, regardless of any remaining inactive artefacts (Latour 2005, p.53). ANT wishes to liberate the actor, its individual actions and success in recruiting allies and forming associations without attempting to force them into a role (Callon and Latour, 1981). A researcher must therefore examine any rise of professionalism by engaging with those who seek to be spokesmen for the general population, rather than simply assuming every security manager adopts an aligned desire upon signing their contract.

3.5.2 Action

The non-purposive, non-sentient or unaware actor is explained by the assertion that the actor is not themselves the source of an action but is *that which is made to act* at the nexus of other entities (Latour 2005, p.46). Again, the ambition is to remove the assumption that actions are caused by a pre-determined range of social forces which constrain the individual, who must then rest in an accepted groove. The study must reject the concept that “a profession” acts in a unified way and see this instead as individuals organised to act in concert by some action. As seen below, commentators such as Walsham (1997) suggest that a *wholly* local approach rejecting pre-made social “forces” can lead the observer to overlook the effect of outside influences; those seeking greater depth to theory were invited to consider Structuration Theory (see also Johnston, 2001).

3.5.3 Objects

Society, as mentioned above cannot be accepted as an externality – a pre-existing force shaping the lives of its constituents – but must be treated as the result of actions to render established associations more durable. Objects participate in action (Latour 2005, p.70). The “actor” in ANT must be independent and have the ability to surprise. They cannot merely be a “mere intermediary” functioning as a push-rod, they must play a part in action and leave a trace. Latour (2005, pp.37–42) states firmly that anything whose work is not visible cannot be an actor. An actor is frequently itself a “punctualised”⁵ assembly (Law, 1992), something briefly constructed from its constituent parts.

⁵ as in *made into a point*, or appear as if a single point

3.5.4 Facts

Latour (1987) in particular proposes firmly that facts are *black boxes* which form as a particular theory gains acceptance. That which today is an “unproven” theory of one research federation and the subject of robust debate later, after it has gained acceptance becomes “true” and axiomatic without further discussion. That humans are now seen as central to security rather than viewing the subject in entirely technical terms is an example of such a transformation.

ANT seeks to open these black-boxed facts to enquire how they were formed or to watch their creation or decline. An analogy is given (Latour 1987, p.30) of the passage of a parliamentary bill – the fluid focus potentially of considerable debate, controversy, persuasion, politicking and eventually the recruitment of a sufficient number of allies whose interests one way or another appear to be advanced by its enactment – through to being a solid piece of legislation, handed down as unarguable, enforceable law. Like justice however, the settlement of a controversy into a fact must be “seen to have been done”; the settlement must be visible and mobilised by others as fact in later controversies to be considered stable (Latour 2005, p.40). This effect is evident in the stabilisation of the BS7799 security standard (as was) from highly political and controversial proposal to well-accepted global benchmark (Backhouse *et al.*, 2006).

3.5.5 Descriptions

An ANT study is a description of a network caught at a moment in time– an account of the visible products of actors’ work “where all the actors do something and don’t just sit there” (Latour 2005, p.128). Without the pre-fabricated social forces which can be used to explain the observed phenomena in terms of the expected, the actors must be followed and their empirically visible traces and their results described. Networks are however potentially infinite; a somewhat arbitrary boundary must be drawn according to the resources at hand and the space available to report the findings (Latour 2005, pp.121–148).

3.6 Moments of Translation

An Actor–Network is a “heterogeneous network of aligned interests, including people, organizations and standards” (Walsham, 1997). ANT accounts describe the process whereby an entity becomes the exclusive spokesman for the interests of other actors who accept them as the gateway to satisfaction of their own interests (Callon, 1986). In ANT’s most important methodological work, Callon (1986) distilled the stages (“moments”) of translation into four steps.

3.6.1 Problematisation

ANT is concerned with action, thus it is frequently used to describe the formation of a set of alliances which developed into an Actor–Network. The actors themselves are identified and their interdependencies established. For the formation of a durable network, the actors must come to accept that their various interests are advanced through some process on which they all rely, an Obligatory Passage Point (OPP) as illustrated in Fig. 6. This requires these problems to be framed in such a way that the *focal* actor can make an offer to assist the others through an association with them.

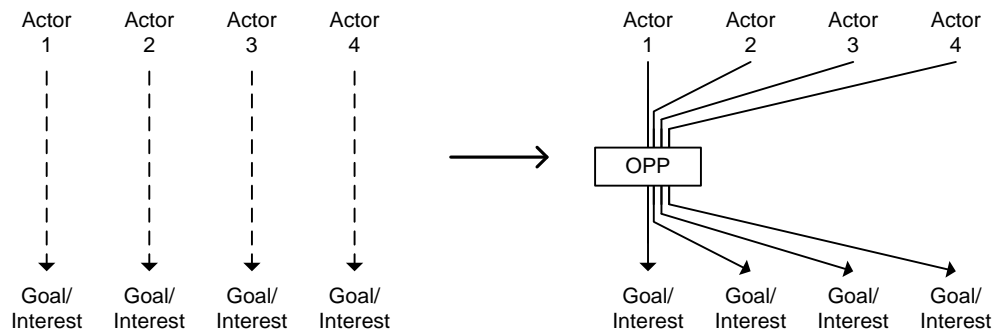


Fig. 6: Illustration of OPP formation, from Callon (1986, pp.206–207).

Problematisation thus “describes a system of alliances, or associations, between entities, thereby defining the identity and what they ‘want’” (Law 1986, p.206).

3.6.2 Interessement

Once the actors are defined, an actor hoping to become a spokesman for the entire network must begin interesting the others in their work. Simultaneously they begin divorcing them from any rival actors which allow an alternative route to the state being offered (alternative passage points). A campaign of sorts is undertaken (through *devices*: tactics or some physical entity) which lobbies the actors to be recruited to the endeavour. The attempt is – through negotiation – to align the actor’s interests with those of the putative spokesman and hence consent to the alliance and strengthening the emerging network. This process is the incarnation of the concepts advanced during Problematisation (Callon, 1986).

3.6.3 Enrolment

If Interessement is successful, the various actors will be *enrolled* by the focal actor (Callon, 1986), in that they will consent to the alliance and accept their roles in the network and donate

their own capabilities to supporting it. Callon is quick to point out that these are not roles in the sense of generally accepted societal positions; rather this stage defines what each actor does and wants and how it relates to the others. The actor allows himself to be represented by the focal actor as a “spokesman” for the aligned group’s interests.

3.6.4 Mobilisation

“An actant can gain strength only by associating with others.”

(Latour 1988, p.160)

Representation of those mobilised may be indirect, performed through negotiation with a spokesman. Such a spokesman may be a representative as traditionally understood (such as a union shop steward), the representation of a subset of objects through a sample or the presentation of a set of actors’ interests through a mouthpiece such as the representation of the behaviour of some object through a figure or instrument. This facilitates the mobilisation of a large number of allies to a cause through that figurehead, however this only holds whilst that support continues (which might be checked using a test of strength and whilst the spokesman does not betray the represented through self-interest, or at least is not found out).

“In our definition the crucial element is not the quality of the represented but only their number and the unity of the representative”.

(Latour 1987, p.72)

Callon (1986) mentions the comparison of a spokesman as a political form of induction, the assumption that where one leads all will follow.

3.7 Success

A project, according to ANT, succeeds or fails on the basis of its ability to form a sufficiently durable alliance of interested parties who have been convinced that the project is the gateway to advancing their own interests. In Latour’s (1987) language, the price of dissent is raised by accumulating so many allies for which one can speak (and who can be protected from poaching by the challenger) that it is impractical to form a counter proposal.

Dery *et al.* (2013) note that the “neat” process above as described by Callon (1986) is not necessarily seen empirically in a perfect linear and sequential fashion thus success may only be visible after several attempts to fulfil the stages identified. Gonzales and Cox (2010) by way of example present an account of HR process implementation which partially failed due to lack of enrolment of key actors. An ANT account does not look at the morality of the movement, whether it is in general terms “beneficial” or achieves an externally-imposed success criterion

(Scott-Smith, 2013) but simply aims to describe the formation of the alliances through which the various interests are mobilised.

3.8 Criticism

ANT is not the work of a unified political organisation with a well-polished party line; it has evolved and developed through debate and even fracture (Walsham, 1997). Proponents and critics of ANT (not necessarily exclusive groups) have argued at length on the topic and it is not proposed to fully cover the area here, however some note must be taken of the limits of certain concepts.

The “symmetry” of treatment of human and non-human actants in terms of agency or ability to cause action is probably the most controversial aspect of ANT, even though the intent to introduce the non-human generally has had overall success (Sayes, 2014). Perhaps the most well-known criticism of the symmetry was by Collins and Yearley (1992) who, pointing to the absurdity of that symmetry taken to extremes, prefer to advance and retain the differentness of human intention. As many have noted (see McLean and Hassard (2004) for a useful summary) the principle of symmetry is useful in reminding the analyst that whilst humans can make strategic decisions – albeit as Callon (1999) notes, not all actors are in a position to make perfect choices with a full view of all available strategic options – non-human entities can cause effects and take their place in the network surrounding those human choices and acts. “Action” in this sense however is not a straightforward statement of direct intentional cause (Latour 2005, pp.70–72; Johnston, 2001).

Following the argument of Callon and Latour (1992), it is accepted that the position of ANT is a reaction to a sociology of human separateness and specialness which underplayed the interactions of heterogeneous materials and that the extreme equivalence positions alleged by some critics are straw man arguments. There are clearly differences of agency and intent between human and non-human, however it is not accepted *a priori* that all interesting events and translations inside the Information Security network – which is so completely dominated by the effects of and changing possibilities created from technological change – are the result of deliberate human action.

Further criticism must be answered concerning the lack of taking a moral position or judgement. By taking no stance on the motivation of the action and concentrating purely on describing it, it is possible to level accusations of relativism; much of the criticism of ANT has centred on this lack of moral comment (see Winner, 1993; Amsterdamska, 1990). On the point of ethics, Law (1992) notes that this is an analytical position only which seeks to recognise the involvement of

objects in the networks which shape behaviour, which does not seek to make human and machine morally equivalent. As explored by Johnston (2001) it is possible also to consider some automatic processes which favour a given outcome (such as evolution) to be thus *intentional*, even if not rational or strategic.

Callon (1999, p.193) characterises some of the criticism as centred on the actor as “guided by the quest for power and solely interested in spreading networks and their influence” (see also Latour’s (1999a) defence). Indeed, the actor may have no intention or motivation and be enrolled by others (Callon, 1999). Studies using ANT have however been published which show a moral angle; some (such as Latour (1991)) argue that it is possible or indeed necessary to use an apolitical tool to describe a network before making a judgement. That emphasis on adopting no *a priori* assumptions about the nature of associations between entities which must be traced carefully and empirically arguably makes ANT a firmer basis for Critical studies to examine relationships of concern (Doolin and Lowe, 2002). Moreover, this study sets out to examine the state of a network but has no “mandate” from its title question to seek to cast judgement except where analytically necessary, therefore an amorality argument does not deter here.

3.9 Actor–Network Theory in Information Systems and Security Studies

ANT has been found increasingly to be a useful approach in some computing studies (Cordella and Shaikh, 2006) due to its refusal to allow a distinction between the “material” and “social” worlds, which are inherent parts of any IS study (Tatnall and Burgess, 2002). It seems at least superficially well suited to a study at the nexus of human–computer interaction since it rejects the concept of a boundary, seeing only patterns in associations between entities (Law, 1992; Latour, 1999a). From an ANT perspective, whilst it is possible to draw a boundary around the physical machinery which runs a new piece of software, it is impossible truly to distinguish which parts are “entirely technical” which are not the result or driver of some interaction between other actors (Tatnall and Gilding, 1999). As discussed above, Walsham (1997), although no eager proponent of ANT, suggests that although the full symmetry of technical and human actor need not be accepted to make use of the concept in IS studies; it is not a coincidence that such a theory should have arisen within the “increasingly complex socio-technical world in which we live” and the compatibility of the approach with this study is in accord with this statement.

ANT remains a popular and valid approach in this area. It was used well by Dery *et al.* (2013) for example to show how the competing interplay of interests can explain “surprises” not otherwise predicted by solely technical models. Similarly, Wang *et al.* (2015) used ANT as a lens as part of an investigation into the Chinese mobile telephony market to enrich the

identification and description of key interactions. The elements of competition to enrol others and the consequent unpredictable nature of network formation according to different levels of success of different interests were used by Rhodes (2009) in an interpretative study of IT systems in Africa. Díaz Andrade and Urquhart (2010) similarly employ ANT as a lens and use it to structure the report into the stages suggested by Callon (1986). In another interpretative study, Cho *et al.* (2008) use ANT to examine particular moments (events) where translations occurred during the implementation of health systems.

The relevance of ANT to Information *Security* topics was demonstrated by Hedström *et al.* (2010). They convincingly describe the hacking of a university computer system in terms of an Actor–Network where the aims of the security function were incompletely translated. An approach which favoured a purely technical solution to security problems over negotiating with human actors, coupled with an assumption that the network once formed was static rather than fragile and temporary, fatally undermined the network’s ability to defend itself from rival focal actors (in this case, the hacker). Whilst inscriptions were produced in the shape of policy documents, these were not successful in convincing the free actors to align with their substance and commit to the cost of maintaining the required discipline. Komatsu *et al.* (2013) demonstrate this empirically, showing that a rational or claimed intention to behave securely does not always translate to decision-making in the general user community.

Guo (2013) goes on to show how these networks are highly complex; underestimating the interaction within the network or presenting it in simplistic terms is unwise and led to flaws in pre-behavioural security literature and approaches. Bonner and Chiasson (2005) traced such a network describing the adoption of Fair Information Principles as a privacy standard which became itself a black box within a network.

As an example of work attempting to explain the divergence in theoretical perspectives on security strategy, Seeholzer (2012) identified multiple strategies for organisations, ranging from clients of standards or best practice documents and procedural approaches, authoritarian power-based policy execution through to merely portraying secure behaviour for public consumption. From this it is evident that the motivations behind the behaviour of companies are varied and complex.

3.10 Summary

The professions are most effective when they can be seen as collapsed single actors or “black boxes” (Law 1992), consisting internally of professional bodies, curricula, schools, their members and others (Abbott 1988, p.79-83). ANT’s concept of irreversibility is key here as it

has a strong analogue with the professional goal of achieving state-sanctioned monopoly. Using Callon's (1986) terminology, the professional body, using credentials of competence as devices of *interessement*, persuades the state that it is an OPP to proper regulation of the industry by enrolling and acting as the spokesman for the professionals, who are mobilised in supporting its claim in order to gain status and wealth (illustrated in Fig. 7).

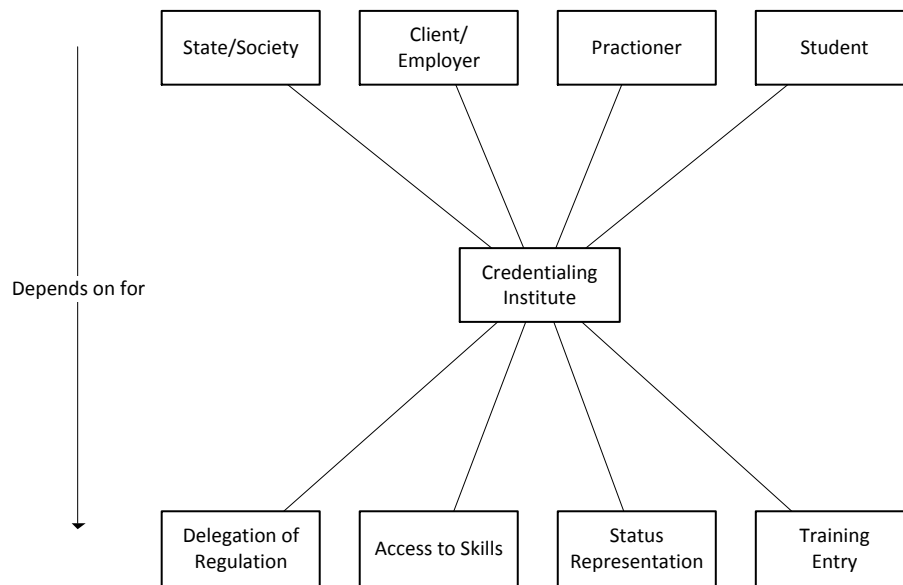


Fig. 7: Credentialing institutions as a possible “Obligatory Passage Point”.

According to Abbott (1988, p. 93-97) this network might break down in two ways, either externally where expanding domains cause a new area of practice to appear where professions compete to fill the void of occupational control, or alternatively the professionals within the point actors (the professions) may feel that they no longer wish to be represented by the existing professions, thus their internal networks may split to create new professional groups (as seen in Fig. 3). ANT is clearly appropriate for an account which must account for and support the agency of both technical and social factors. ANT's core concept of pragmatism toward the physical form of actors – treating human and non-human symmetrically (Latour, 1987; 2005; Law, 1986; Callon, 1986) – is similarly clearly applicable.

Aligning ANT with the overall interpretative approach and placing it in the paradigms described at the head of the chapter is not straightforward. Whilst some writers such as Rhodes (2009) have published full ANT studies as interpretive without qualification, describing ANT as an interpretative approach is not without controversy. Whilst it is often deployed as a lens within an interpretative study, interpretivism is associated with an ontology where reality is constructed subjectively. ANT, on the other hand is concerned with tracing but not judging the movements of multiple actors as they form and reinforce structures through their actions, thus in its purest

form ANT is arguably positivist and realist (Whittle and Spicer, 2008; Cordella and Shaikh, 2006; Elder-Vass, 2015). Similarly Bird (2009) notes that whilst interpretivism “has a constructivist ontology”, ANT insists that the actors are free to express themselves and the researcher must not put words into their mouths (see Latour, 2005). The researcher, by adopting an interpretive stance is, to Bird, forcing the actor into their constructed universe through controlling the medium of interaction. It is difficult to see however how this is ever avoided in any non-positivist study, there always being an element of interpretation, and must surely be accepted as an inherent part of the research process and limitation of the degree to which that philosophy can shape research in its purest form. As Johnston (2001) notes, even which actor is the focal entity is a choice of the analyst.

In reality, any account must at least summarise and reduce the data, and to have any relevance comment upon it. Therefore it is accepted that ANT must be seen as a sensitising concept rather than an absolute and pure philosophical position: the “lens” approach criticised by Cordella and Shaikh (2006) as importing concepts from but not recognising the realism implied by ANT. Since it was seen above that a profession means little without recognition of its status, its certifications mean little unless they can be used to cause an effect, and even the concept only exists in those societies where such a “special trade” has meaning; it is clear that “profession” is an entirely constructed concept. Whilst pure ANT would regard the reality of a profession as constructed in the interplay between the elements, since that interplay only ever has meaning in symbols and attitudes it is difficult to imagine an interesting or useful account of the construction of that meaning in this context which does not include a degree of interpretation through the author’s inevitably filtered vision (McLean and Hassard, 2004; Collins and Yearley, 1992). Thus ANT will inform the analysis and shape the research questions in several ways:

- It has been seen that many developments have influenced the ability of a (more powerful) security profession to form, such as the creation of standards, the maturation of the discipline, the emergence of human-centred governance topics and the increasingly severe threat to business viability from the emergence of malicious code and actors. It is not clear whether these are themselves the works of actors, the devices which have been used to mobilise others to the cause of a particular actor or they themselves are actors. ANT and Abbot’s theory of the “System” of professions jointly form an interesting and useful perspective for analysis.
- The questions surrounding the origin and intention of the profession, the identification of the actors as separate from the inert, the openness to the non-human (especially in such a highly technical domain) as a source of those actors, together with the element of

intentionality flow from taking an ANT perspective.

- The epistemology and methodology are also informed by the principle of following those actors, identifying them by observing their traces (for example in understanding their motivations and their view of the significant actants which competed to represent them).

When the results of each question area have been presented separately, the general discussion will aim to draw a description of the movement towards professionalism if this is indeed observed from the data. The findings will be presented from an ANT perspective but interpreting the meaning and acceptance of the symbols seen in this constructed entity of “a profession”.

Chapter 4: Methodology

4.1 Introduction

This chapter considers how most effectively to respond to the research questions by justifying the experimental approach taken and the selection of the most appropriate method for data gathering and analysis. The data gathering section begins by reflecting the epistemological choice described in the last chapter and using this to show how those methods which do not produce the types of data desired were excluded, as an initial filter. The basic research design is then discussed, followed by a consideration of which methods are compatible with the positions chosen. After noting issues of methodological consistency and practical considerations the chapter then compares the candidate methods and details the approach proposed prior to entry into the field.

Following this, the chapter then presents a report of the work as carried out, including the ethical issues raised, lessons learned during the pilot study, the recruitment of participants, the creation and adaptation of instruments and the analysis steps used in the following chapters.

4.2 Data Gathering Methods

The following section considers the candidate empirical methods, considering first the types of data to be gathered.

4.2.1 Qualitative and Quantitative Data

The first question concerns the type of data to be collected, although in practice most studies can usefully include methods which collect both textual and numerical results and validly present results in either format (Remenyi 2012, p.2). As Myers and Avison (2002) noted, there is also no completely inflexible link between a particular form of data and a particular paradigm. Whilst positivist studies may frequently wish to use numerical data to confirm that a hypothesis is highly likely to be true, positivism is entirely compatible with the use of qualitative data (Walsham, 1993) and neither is inherently superior.

Originally, qualitative approaches were seen as non-systematic or non-rigorous. They were tools to explore a new area where there was no theory available to explain observations or possibly to guide what should be observed. Once a plausible explanation had been imagined which appeared to fit the facts, this could then be turned over to “more solid” quantitative techniques for scientific testing and verification (Glaser and Strauss 1967, p.16). There is now more

agreement that the two are complementary and a pragmatic approach can be taken to applying methods on the basis of applicability to the research question (Flick 2009, p.32; Silverman 2000, p.1; Dhillon and Backhouse, 2001; Myers and Avison, 2002).

Whilst it is sometimes the case that quantitative work is seen in natural science circles as the superior form (Flick 2009, p.25), representing the trial of the qualitative hunch in the rational and objective court of proof, both types of research can be applied inappropriately and performed badly, thus neither selection lowers the requirement for rigour, consistency and a systematic approach (Silverman 2000, p.12).

4.2.2 Compatibility with Overall Paradigm

The design of experimental method reflects the epistemology with which it is most often associated. Positivism, with its emphasis on rigorously measuring and testing, will tend to prefer reproducible studies whose output can give a reliable judgement of how well a hypothesis matches reality. Conversely, an anti-positivist epistemology, which favours a rich description of the respondent's view, will reject a method which repeatedly asks a relatively superficial question. This latter action is well-accepted for determining whether a population acts in a certain way but does not explore why (Flick 2009, p.16).

The title question is compatible with a functionalist approach if it could be established that there is a metric for testing whether professionalisation has succeeded, however no such scale is universally accepted and in any case such a study would be unsatisfying at the level of explanation. This research adopts an anti-positivist position and seeks to form a deep understanding through a rich explanation of individual cases and allowing actors to speak in their own terms. The strategy was thus to seek methods which allow freedom for the participants to answer freely without imposing a structure of pre-determined acceptable answers and thus the following three classes were rejected.

4.2.2.1 Forced Choice Methods

Popular sources of quantitative data for social studies are forced-choice surveys: questionnaires and structured interviews (Bernard, 2000). With limited resources, collecting data through automated means such as an online survey would be highly efficient as no per-respondent time is required from the researcher. It is also useful for capturing data quickly within a fixed time frame, such that the answers of the later interviewees are not shaped by an event reported at some point in the fieldwork. Impersonal methods prevent the interviewer from unintentionally steering or indicating the "correct" answer, subject fatigue affecting the attitude of the

researcher or the participant being affected by how they perceive or react to the researcher (Bernard 2000, p.230).

A key benefit of forced-choice approaches in positivist studies (which will frequently present correlations in numerical data statistically) is enabling generalisation, since random sampling and statistical weighting can be used to ensure that the conclusions are as generally applicable as possible (Bernard, 2000). This has particular relevance here in terms of claiming to represent the larger population. These techniques are also very widely accepted with well-established methods for analysis and presentation, potentially making defence of the study more straightforward.

As discussed below, the sensitivity of the subject matter could have influenced participation; refusal rates reduce according to the perceived “threat” of the questions, although the perceived anonymity and reduced tendency to alter the response to impress or avoid the moral judgement of the interviewer gained from a self-administered instrument can reduce this effect (Bernard 2000, pp.229–232) which was seen as a potential benefit.

Ultimately however, whilst this would be highly fruitful for studies adopting a different paradigm, such a method would be extremely difficult to adopt whilst still complying with the strategy of allowing the actor to generate their own ideas and signify their own concepts of what is relevant and these approaches are rejected as incompatible with the epistemology. As Drever (2003, p.3) notes, with such techniques “you never learn anything you didn’t ask”.

4.2.2.2 Laboratory Experiments

When attempting to demonstrate a correlation between variables, it is necessary to control the environment to hold equal or account for all other factors. Controlled conditions are excellent for removing external influences, however for the same reason laboratory experiments are poorly applicable to areas involving risk, judgement or decision making (which clearly applies here). Galliers and Land (2002) cite two reasons for this:

- It is not possible to accurately model the selection of real world actions under conditions where the pressures, stress and variable amounts of information completeness do not apply, and
- The introduction of metrics requires the elimination (or treatment as irrelevant) of those aspects which are difficult to quantify but which do have an influence.

As above, attempts to investigate and isolate the pre-determined factors under study prevent the subject being the generator of their own truth.

4.2.2.3 Action Research

“Action research aims to contribute both to the practical concerns of people in an immediate problematic situation and to the goals of social science by joint collaboration within a mutually acceptable ethical framework.”

(Rapoport, 1970, cited in Myers and Avison, 2002)

Action research originated in the 1950s as a method for conducting psychological research. It involves two stages: firstly the researcher collaborates directly with the subjects to diagnose a problem (develop a hypothesis), then addresses the issue based on that hypothesis. Although popular in Education (Berg, 2004) it has generally not found favour in IS studies (Baskerville and Wood-Harper, 2002); a notable and relevant exception is the study of policy compliance awareness training by Puhakainen and Siponen (2010).

The strategy has some parallels with ethnography in that it involves sustained single-case participation, however it centres on collaborating with the subjects with a particular practical outcome in mind to improve the lot of an identified group. Whilst this emancipatory model of undertaking research which itself effects change would be particularly compatible with the aims of much Critical Theory work, Olesen and Myers (1999) adopted an interpretivist position within Structuration Theory and noted the theoretical kinship with ANT (see also Atkinson and Brooks, 2003). It is arguable however that without the element of change present in the research aim, the “action” aspect becomes somewhat moot. Since no requirement to effect change exists this approach was rejected.

4.2.3 Basic Research Designs

Having rejected incompatible classes of method, it is appropriate to turn now to design. Flick (2009, pp.127–145) suggests four basic designs: retrospective, snapshot, longitudinal and comparative. Each will now be considered (and illustrated in Fig. 8) and their potential in this study discussed.

4.2.3.1 Snapshot Studies

Snapshot designs capture a state of affairs at a particular moment in time (Flick 2009, p.137). This is something of a *default* as the investigation of a topic “as it is found” is clearly a natural approach to inquiry.

4.2.3.2 Retrospective Studies

Retrospective studies attempt to reconstruct a historical case (often biographical using narrative methods) to elicit data on some significant event or process and its meaning for the individual (Flick 2009, pp.136–137). It is not an ideal approach for seeking a highly factually correct historical account given inaccuracy of recall and bias from post-event re-evaluation, the unverifiable and secondary nature of some of the data collected on the influencing events, the selection of respondents and the difficulty of exploring retrospectively the alternative paths which would have been available (Raffaelli and Ontai, 2004; Flick 2009, p.136), but has the advantage of capturing an individual’s point of view.

4.2.3.3 Comparative Studies

These compare specific aspects across several case studies, seeking contrast between them or variation along a particular dimension, holding all other factors as constant as possible (Flick 2009, pp.135–136). This might examine whether particular factors influence professionalisation (such as industry size), therefore elements of this approach could be included. Care must be taken however in an interpretative study not to stray into a positivist perspective of comparing scores on variables whilst controlling for confounding factors; the intention of this study is to examine the cases individually (being essential also for actor freedom in ANT).

4.2.3.4 Longitudinal Studies

Longitudinal studies sample some property repeatedly over a time period sufficient to allow substantive developments to take place to compare observable changes (Flick 2009, p.138). This is potentially a fruitful line of enquiry, as the development of an emerging profession could be repeatedly examined to observe any change in status, professionalisation activity and adoption of credentials or similar standards as *de facto* or *de jure* barriers to entry.

4.2.3.5 Summary

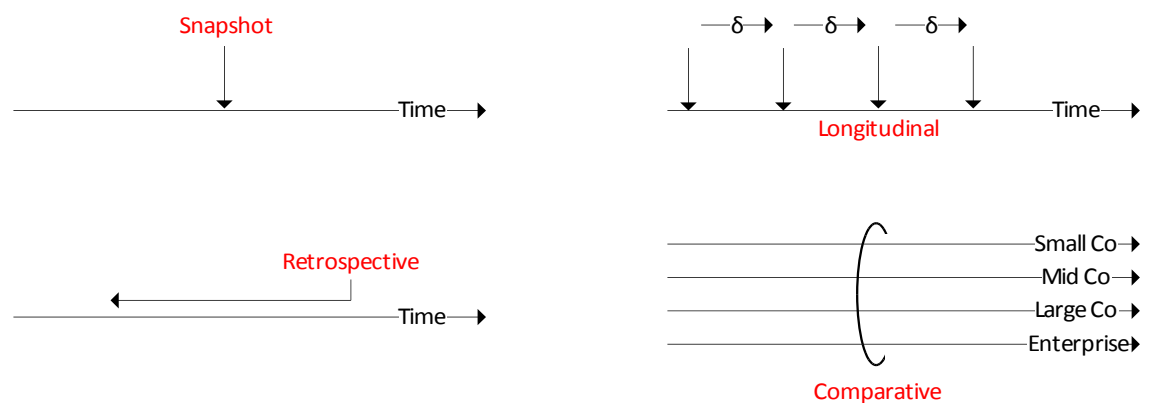


Fig. 8: Comparison of the “basic” research designs, based on Flick (2009, pp.127–145).

The research question asks to what extent something in progress has been achieved, thus the time period considered is highly relevant. It is split into three sections, which map to concepts of origin, current status and future direction. Neal and Morgan's (2000) first two stages of professionalisation – full-time work and specialist training – have clearly begun, thus a retrospective component implied by the element of origin is required.

A longitudinal component is in principle suitable to observe current and future status, particularly coupled to the ANT desire to see actors moving. Professionalisation is however a slow process: Wilensky (1964) and Neal and Morgan (2000) describe professionalisation processes over several *decades*. It is therefore not sensible to attempt observation of such changes during a relatively short study since it risks not capturing any useful output.

Professionalisation can be seen as simply a homogenous movement of the entire community, of like intent and mind but dispersed throughout a range of environments and hence exposed to varying pressures. In this case taking a snapshot of the overall community and examining the interrelationships already built and the motivations of the key actors for the future would have been valid.

Since the actors may not be exclusively people (they could be technologies, standards, legislation, malware or a multitude of others) it might be legitimate to undertake a comparative study to identify these other factors and suggest correlation. ANT discourages pre-selecting which actors the researcher will “permit to act”; any approach which attempts to follow some factors and control for others is therefore incompatible. The project seeks to enquire from the available sources what made them act and identify these other actors during analysis of what is said, rather than deciding at design time what to see.

No *single* design from the above was therefore applicable. The chosen methodology must support a retrospective approach to reconstruct past movement as well as being able to capture the *status quo* and direction.

4.2.4 Candidate Strategies and Methods

The remaining strategies and methods are considered below, before a “suitability and practicality” filter is applied and the remaining options tabulated. From Bernard (2000, p.8), “method” here will refer to a technique which generates data, whereas “strategy” will be applied to the organised execution of one or more techniques in a particular pattern or setting.

4.2.4.1 Case Studies

“A case study may be defined as an empirical enquiry that investigates a contemporary phenomenon within its real life context, when the boundaries between phenomenon and context are not clearly evident, and which multiple sources of evidence are used.”

(Yin, 1989 cited in Remenyi, 2012)

Case studies are a widely-deployed strategy used in qualitative information systems research (Orlikowski and Baroudi, 2002) and widely and increasingly used in Management Information Systems studies (Lee, 2002; Remenyi 2012, p.14). They are often used in situations in which research and theory are at their “early, formative stages” (Cepeda and Martin, 2005) as was seen in the literature review. Collection of any form of data is possible and the approach is compatible with any epistemology: it can be used develop theory or to test it in the field. Multiple case studies may be performed in order to provide contrasting data and deepen the scope of the study, although this does not equate to “generalisability” comparable to a large-scope random-selection survey (Remenyi 2012, pp.5–13).

Case studies were in principle a highly promising strategy for this project. It was shown above that professional status is subjective, in the gift of the beholder. A potentially fruitful avenue of enquiry would have been to explore the interfaces for interaction illustrated in Fig. 9:

- The professionals themselves: do they consider themselves part of a profession and do they consider themselves separate from IT?
- Their IT colleagues: do they similarly recognise the separateness of the discipline?
- Their employers: are they accorded status and respect by their clients?
- Their would-be peers: are they treated as peers by established professionals?

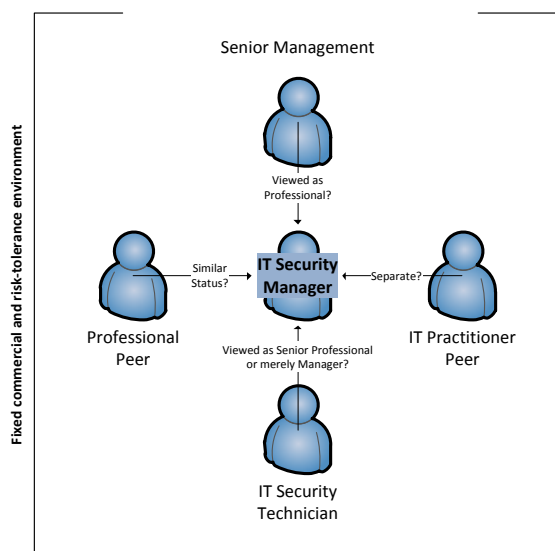


Fig. 9: Possible relationships explored in some potential case studies.

The context of practice for each respondent however would be different, introducing inconsistencies in the comparison. It was noted, for example, that the power of the security function can vary according to size and which legislative pressures are present, but could also vary according to factors either not or only weakly identified so far. Brady (2007a; 2007b) claims that IT professionalism varies internationally, thus it would be necessary either to acknowledge nationality as a variable (which presents practical issues of expense and language) or, as was the case, acknowledge the limitation of the work being UK-centric research.

Even if it might be possible to limit those variations known and considered at the outset, at present the enumeration of such factors in the literature is incomplete. Thus case studies would be useful in ensuring that all respondents in one study are fixed in a particular context. Any exploration of where such variances are to be found could then have been guided by both theoretical sampling (Glaser and Strauss 1967, pp.45–77) and the two advance directions mentioned above (Flick 2009, p.116). Whilst generalisability is a potential problem for such research (see below) this would certainly aid reliability since it allows for a greater number of responses than a single case.

In each case, representatives of each group could be interviewed on their impressions of role and status of several professions, including the more established examples also found in that setting (e.g. accountant) and the IS profession for comparison. Given that there is a comparative element, any data collection would need to be at least partially structured, however since the respondents must not be led and there would likely be great interpretive flexibility there must be some freedom to explore the perceptions of each person.

4.2.4.2 Ethnography, and Direct and Indirect Observation

It is common to immerse the researcher into the culture of the group being studied and their environment (Flick 2009, pp.222–238; Bernard 2000, pp.318–409), typically over an extended period of time with one year being typical (Bernard 2000, p.318; Cresswell 2009, p.13). This strategy emphasises validity through ensuring the researcher is properly grounded in the data whilst remaining as objective as possible (Bernard 2000, pp.324–325).

Some of the output of a security manager is public textual product, for example policy, however this will be the negotiated product of a political process. In assessing professional status, observing the negotiation of that output would be relevant, since it would be a test of power to determine (for example) how much of the manager's desired text passed into the final document against resistance. Without a prolonged case study producing highly developed knowledge of the culture of that organisation it would be difficult to know how controversial the proposals are

to others in that culture (and thus how successful the manager needs to be to drive them forward). It would be difficult to remove elements such as effectiveness derived from a practitioner's *personal* qualities from the status of the profession they represent, if these are even separable.

This would therefore in principle be valid, although a major question would be whether sufficient breadth of data could be amassed in order to make it useable beyond the context of the specific study. This question of generalisation or transferability is discussed below.

As an aside, immersion into the world of the subject does have a number of wider benefits. Bernard (2000, p.325) for example believes that increased familiarity and trust can reduce the observation effect of the subject's behaviour changing when they are conscious of being watched, and that a familiarity with the lexicon of those being studied can assist with the development of data gathering instruments. Even if the decision is not to undertake an ethnographic study, the experience of the student as an IT professional working in a parallel field arguably produced some of the benefits Bernard describes.

4.2.4.3 Interviews

The interview is the most common method of data gathering in qualitative research (Myers and Newman, 2007). Flick (2009, pp.150–172) lists several forms.

4.2.4.3.1 Focussed

A uniform stimulus is shown to the subject (such as a film or piece of literature) and its effect noted through a series of related questions (Flick 2009, pp.150–152). No such stimulus particularly suggested itself for this subject which would helpfully focus an interview on the selected topics, thus this method was not considered.

4.2.4.3.2 Unstructured

Here the interviewer does not strictly refer to a schedule of questions and minimises the control exerted over the interview direction by the interviewer. They are not simply informal conversations however since the interviewer still maintains a direction of interest rather than engaging in natural dialogue (Bernard 2000, pp.191–195), which is highly aligned with the ANT approach. Biographical or narrative accounts may benefit from a looser structure, however as the respondents had limited time during a single interview and some inter-session comparability was required for drawing contrasts and general inferences, a more structured approach was considered the better choice (Bernard 2000, p.191).

4.2.4.3.3 Semi-Structured

This is the most common type of interview in IS research (Myers and Newman, 2007) and is seen regularly in work with a similar intent to this study, for example that of Werlinger *et al.* (2009). It is centred around a guiding instrument to provide a spine to the discussion and ensure that required topics are addressed, but allows for exploration of emerging points of interest. In addition it has the practical advantage of efficiency and is thus useful for interviewing busy professionals who will expect efficient use of time (Bernard 2000, p.191). As a widely deployed method, it carries the advantage of precedence, aiding design acceptance by a reader familiar with the field.

The ANT lens requires giving freedom to the actor to express their view of their professional environment and its formation, whilst concerns of generalisability or transferability (discussed below) requires that at least some structure is present to aid comparison and rigour in the approach. This method thus had considerable potential, either within a wider strategy (as a tool during a series of case studies) or as a standalone method.

In its standalone form, this method has particular application to the examination of the current status of the professional, by interviewing both themselves and potentially (as discussed under “Case Study”) those who interact with them. For those with sufficient career history, it allows access to views on the formation and future of the profession, allowing them to nominate their own actors in the network (their memory represents the necessary *traces*). The future of the profession could also be addressed with those seeking to advance the profession, for example those in computer societies and credentialing institutions. These could be seen, in an ANT sense, as attempting to form an OPP as spokesmen for the profession. Such people are (in contrast to the general security worker) likely to have relatively well-developed views on professionalisation of the industry and advanced knowledge of current developments in the area.

4.2.4.3.4 Expert

People with highly developed knowledge in a particular subject area can contribute either by supplying specific insights or information, or by validating or interpreting information learned from others. They are supplying information in terms of that expertise and not in their private role. Care must be taken in the preparation and execution of the interview protocol to avoid the expert taking a lead role in the discussion and moving the topic to their own areas of interest rather than the interview subject (Bernard 2000, pp.165–169).

This method could be used as triangulation in the “corroborative” sense described by Bernard

(as exegesis or confirmation of the conclusions in the analysis of accounts given by others), however this description might also validly apply to interactions with those seeking to advance the professional state of Information Security workers described above. These would however qualify only partly as “expert” interviews according to Flick’s (2009, pp.165–169) definition, since the respondents are experts in the subject area, however as proponents of professionalisation they are not wholly disinterested informants and the study is interested in the views of the person in these aspects (as spokesmen for their organisations and therefore potentially for the practitioners they wish to enrol).

Whilst not all professions attain or even aspire to legal protection for their monopoly, professionalisation movements tend towards seeking sanctioned jurisdiction (Abbot 1988, p.71). Therefore as well as the viewpoint of those who are candidates to seek that status and those who agitate in that direction, the state is the ultimate grantor of jurisdiction and thus its attitudes to the industry are also very highly relevant. Another source of quasi-expert interview is thus that part of government which would regulate Information Security. Fortunately movements had already begun in this area thus identifying a specific target department had become more practical. As above however, whilst representatives of government could be interviewed in their role as experts on government policy, they are also involved in determining what it should be and would therefore not have been *disinterested* experts.

4.2.4.3.5 Narrative

Narrative accounts are useful for investigating a development from a participant’s point of view. “Narration or story-telling is one of the fundamental ways that people organize their understanding of the world” (Gibbs 2007, pp.56–59). The intention is to elicit an extended response using a wide, generative question which suggests several areas which could be considered by the respondent. The interviewer will be less conversational, encouraging the interviewee to continue and to expand on their points until reaching a natural conclusion (Flick 2009, p.178). Flick notes that the account required should not simply be an elongated answer to a question but must include as far as possible an entire story of how a particular event came to be, from inception to completion.

This has potential in an ANT study allowing the respondent’s account to show the traces of actors which formed their local network. Where interviewees possessed the relevant degree of experience, it was considered useful to include a broad-based question concerning which factors led to the creation of their role in their organisation and the formation of the profession in general.

4.2.4.4 Focus Groups and Dyadic Interviews

Focus groups involve multiple participants in conversation. Whilst this can be useful purely for convenience (gathering information from several sources simultaneously), the interactivity itself adds a dimension, exploring the homogeneity of opinions held and how the subjects came to their views (Kitzinger, 1995). Dyadic interviews study interaction in a *dyad* (two person partnership or close relationship) compared to engaging the participants separately (Eisikovits and Koren, 2010). As an example, McGee (2006) considered examining the discourse between a physical security manager and their internal customer. This approach was however rejected due to concerns that these internal customers would be in many cases senior managers thus consistently gaining access to time with comparable dyads presented a design problem.

Any group discussion concerning the professional role of one member was felt likely to inhibit the participants from speaking freely, it being difficult to dissociate the role from the person. In seeking the subjective viewpoint of the various actors, the priority here is to ensure honesty. This has resonance with a difficulty McGee (2006) reports, in that discussion about the status of a profession within the organisation in a case study or interview was difficult to separate from asking an individual for an assessment of their personal success in gaining status, thus likely to introduce issues of either modesty or puffery depending on the personality of the participant. Drever (2003, p.16) suggests that group-based techniques are best reserved for where the group interaction itself is the focus of the research; this was accepted and the approach not considered further.

4.2.4.5 Media Analysis

The investigation of *origin* requires retrospective identification of how IT Security became an important, mainstream topic. Professional status implies acknowledgement as a domain and those practising it must establish at least partial jurisdiction, ideally in public but at least in the workplace (Abbot 1988, pp.59–85). It was theorised that successful separation would leave visible traces in the IT press, akin to a longitudinal study but without control over the data collected. As Abbot (1988, p.61) observes, the general public may not be able to understand a nuanced separation (since to the layman, all doctors are doctors) however within the parent field, sufficient knowledge should exist wherein this contest could occur. The emergence of security-focussed academic journals similarly would reflect the claim to a specialised common body of knowledge. Walsham (1995) for example, sympathetic to Latour's (1987) view of the construction of scientific facts, sees journals as enrolment devices where editors exert control over a network. As records of security controversies settling into facts they are therefore well placed and much potential was seen here.

4.3 General Factors Affecting Methodological Selection

In the preceding section some candidate data gathering methods were listed, those less suitable for epistemological or practical reasons identified and those with most potential noted. Before a selection can be made however some further factors must be taken into consideration: *methodological* and *practical*. The former ensure that the research output can be accepted according to the conventions and standards of the applicable literature, whilst the latter ensure that no undue risks are accepted which might prevent the project from being completed successfully.

4.3.1 Quality Considerations

Three areas from methodological theory require some discussion in the context of an interpretative, qualitative study to ensure that the research is of publishable quality, which introduces some concepts which will shape the research design.

Three aspects of research quality are routinely assessed for quantitative work in the positivist tradition:

- Validity: the degree to which the research correctly captures and reports the reality of the phenomenon being studied.
- Reliability: whether the results of the study would be consistent if repeated elsewhere.
- Generalisability: whether the findings apply to any group wider than the subjects of the study themselves.

(paraphrased from Gibbs 2007, p.91)

Applicability of these quality criteria to qualitative work is controversial. Assessing reliability through consistency of results for interview data for example is problematic, since each subject will be explaining their subjective viewpoint, thus comparing responses will always be inexact. Exact repetition between respondents might even be deeply *suspicious* and be suggestive of learned or somehow replicated responses (Kirk and Miller, 1986 cited in Flick 2009, p.385). Procedural reliability can however be assessed to ensure that gathering and coding is done consistently and validity increased by referring the interview back to the respondent for confirmation (Flick 2009, pp.386–9).

Frameworks have been suggested for assessing quality in qualitative research, adopting functionalist [positivist] (Lee, 1989), interpretive (Cepeda and Martin, 2005; Klein and Myers, 1999) and Critical (Myers and Klein, 2011; Riege, 2003) paradigms, although these sources

focus particularly on case studies. Studies taking an interpretative approach using primarily qualitative data for theory building (in other words those not looking to prove a hypothesis) can arguably not be assessed on the criteria above and instead these concepts should map to more suitable alternatives, shown in Table 2.

<i>Positivist Term</i>	<i>Meaning</i>	<i>Anti-Positivist Equivalent</i>	<i>Meaning</i>
Validity	Accuracy of capture	Credibility	Conclusions coherent and justifiable from the data
Reliability	Consistency of capture	Dependability	Procedures appropriate and correctly executed
Generalisability	Represents the general case	Transferability, Usability	Results able to be used or relevant beyond the immediate setting

Table 2: Comparison of positivist concepts with anti-positivist analogues (from Remenyi, 2012 p.21; Flick, 2009; Riege, 2003).

The requirements to produce credible, dependable and transferable data are noted and taken forward into the final selection, however before proceeding, some more detailed consideration is needed of *triangulation*, sometimes suggested for increasing credibility, and *generalisation* when discussing populations in interpretative work.

4.3.1.1 Triangulation

The potential of any specific method is finite, therefore some studies aim to enrich data-based theory using triangulation of multiple methods (Flick 2009, p.444). The ultimate expression of this is the *pragmatic* approach, where methodological purity is disregarded and the researcher uses all available resources (Creswell 2009, pp.10–11).

Denzin (1978, cited in Jick, 1979) defines triangulation as “the combination of methodologies in the study of the same phenomenon.” It is an attempt to compare data from multiple types of studies in order to improve the reliability of the conclusions or theory drawn from it. This can be differentiated as “within-method” or “between-method”. The latter refers to where discrete methods are employed but the data sets are comparable, such that multiple views of the same object produce the same conclusions and hence increase confidence in validity. In contrast, within-method triangulation seeks to examine the same output in multiple ways thus increasing the confidence in the study’s internal consistency (Jick, 1979).

Mixed methods can include combining quantitative and qualitative approaches, to validate or objectively disprove hypotheses raised from exploratory work (Flick 2009, p.30); this is

explored in the next section. Conversely, since social science work is frequently value- and motivation-driven (Silverman, 2000) and more often adopts interpretive approaches (Gibbs 2007, pp.6–7) it may be that rather than validating results, qualitative data may provide causal insights to statistical correlations. Together both approaches can contribute the nomothetic and idiographic angles to the study of a phenomenon (Gibbs 2007, p.5).

In this case, the aim is to provide data for an ANT account, which is itself the presentation of those parts of the participants' stories, views or accounts as the author identifies as the critical stages of some observed action. The selection of those events and interactions, and the extent of the network described, are *inherently* subjective (Collins and Yearley, 1992). The use of multiple techniques purely to improve access to objective truth (as implied by a more Realist ontology) was therefore rejected here. No claim is made to objective determination of absolute social truth by this work, thus it was not felt useful to dilute the available resources by attempting to pursue positivist concepts of reliability.

4.3.1.2 Generalisation

The research refers to a population (the Information Security profession) and the environments in which it operates. In the interpretive paradigm the prevailing ontology denies a universal social “truth”, considering each respondent to generate their own, but as also noted above, qualitative research is expected to be useful and applicable beyond a simple description of a unique case. This creates a dilemma. As Hume is credited with proposing, induction has no basis in strict logic, a problem which requires an act of pragmatic judgement to square (Lee 2005, pp.19–23).

Generalisation can have multiple meanings, which span from a positivist statistical proof at accepted confidence levels to *moderatum* generalisation. The latter is “where aspects of [a specific case] can be seen to be instances of a broader recognisable set of features ... then they can form the basis of theories about process or structure”, thus allowing useful inferences to be drawn without rejecting any proposition which cannot be proven to the satisfaction of the positivist (Williams, 2000). The research design must consider whether to fully make claims for a population, in which case those analytical inferences could form hypotheses to be tested in corroborative quantitative work.

This study tends towards Dhillon's (1995) position that it would be difficult convincingly to combine positivist methods of hypothesis testing and interpretive work based on qualitative data. Whilst it is in principle valid to take the result of one piece of work, formulate a hypothesis from it and test this in a second, it is felt that to pursue this approach *within a single work* shows

insufficient ontological and epistemological coherence. It is surely inconsistent to present an epistemology which presents a nuanced report of its subjects' constructed truth but then immediately attempt to test some simplified reduction of this output to prove its universal correctness. Both parts of the study would have internal consistency and each would be valid, however that which is carried over between them is necessarily altered and partial.

Cross-paradigm triangulation was therefore rejected to ensure coherence of the single study. It was resolved instead to note from a succession of cases what can usefully be learned from them individually and also abstract what can be generally seen. The usefulness of the study therefore rests on the quality and coherency of the narrative produced.

“... from an interpretive position, the validity of an extrapolation from an individual case or cases depends not on the representativeness of such cases in a statistical sense, but on the plausibility and cogency of the logical reasoning used in describing the results from the cases, and in drawing conclusions from them.”

(Walsham, 1993 cited in Dhillon, 1995)

4.3.2 Practical Considerations

Alongside those from theory, further restrictions on method arise from proper assessment of risk and resource to ensure that the chosen strategy is practical and achievable.

4.3.2.1 Sensitivity of Data

Security presents particular challenges for participant-based research. For example, the artificial situation and lack of trust inherent in the execution of an interview might translate to reticence on the part of the interviewee to discuss sensitive issues (Myers and Newman, 2007). Kotulic and Clark (2004) attempted to validate a risk management model by survey, which attracted a response rate of less than one per cent; they concluded this to be a particularly intrusive subject area where approaches with no prior introduction are unlikely to be fruitful. Fulford and Doherty (2003) surveyed on security policy and achieved a slightly higher response rate of just over seven per cent however the design factor which increased the response is not clear.

Access to data was therefore considered a significant challenge for discourse analysis, since access to natural exchanges between a security manager and their clients would be difficult to obtain due to its sensitivity and confidentiality. Analysing the discourse of security managers talking amongst peers would be far less controversial as the conversation would be general rather than specific, however problems have been experienced here also. Bowen-Schrire *et al.* (2004) conducted such research however their analysed text was eventually derived from

interviews rather than genuine inter-subject dialogue due to a paucity of suitable data. The authors noted this as a limitation and the potential for inter-subject data enhancing the study.

Ethnographies would similarly have been particularly challenging. It is difficult to imagine how it would be possible to engage in (or even simply observe) a meeting where security managers were at work without being exposed to confidential or sensitive information. In addition, ethnographic approaches frequently cannot specify at design time exactly what they aim to achieve, which can be unhelpful during negotiations with managers who will usually wish to know the boundaries of the work to which they are agreeing (Harvey and Myers, 2002).

Al-Awadi (2009) found whilst researching security policy in Oman that she did not gain the permission of any of her participants to tape-record their interviews but was able to use the “blessing” of the Omani governmental technology agency to achieve an 81% response rate to a related questionnaire. Conversely McGee (2006) in a study of physical security managers found few problems with recording interviews and reported widespread compliance, which he partially attributed to the novelty of being personally worthy of study. McGee however similarly benefited from support from the industry body which translated to contacts who were particularly interested in professionalisation, something which he acknowledged was a potential factor. Therefore if analysis of a verbatim transcript is required, this principle should be validated during a pilot to confirm likely participant compliance.

4.3.2.2 Risks of Extended Duration of Access to Data

This project was conducted in the part-time learning mode alongside permanent employment. This doubled the total elapsed time between entering and leaving the field and hence enabled more serious consideration of longitudinal studies in terms of the opportunity for subject change. Case or ethnographic studies embedded onsite into an organisation were however impractical unless a very infrequent access protocol could have been agreed, both with the participants and the student’s own employer.

Alternatively an ethnographic study might have been undertaken *within* that enterprise, which would have presented fewer issues of time and access, however this raised its own challenges. Firstly, the fieldwork stage could potentially have lasted several years, presenting a risk that the employment might be terminated for uncontrollable personal or professional reasons (see Harvey and Myers, 2002). Secondly, changes in management attitude, trading climate or other factors could have led to the co-operation being withdrawn. As there would be no comparison study possible unless the change happened at a convenient time and the new employer was amenable, this represented a wholly unacceptable risk that the project would have been

abandoned with a total loss of data. As noted in previous sections, ethnographic and observational approaches were therefore discounted on practical grounds. For similar reasons, longitudinal studies were felt to be impractical along with other approaches which were unacceptably exposed to the risk of losing a long-term commitment to the project, such as participative action research.

4.3.2.3 Finance

As this project was privately financed, this acted as an additional filter on those methods which might be considered, although it was important that this did not prevent the project from answering the research question convincingly and defensibly. A strategy which would have required regular long distance travel would have been problematic. In addition, subject engagements could not be compensated and needed to rely purely on the altruism of the respondent. The risk to the quality of the output cannot easily be mitigated thus must be accepted and acknowledged as a potential deficiency of the overall work.

4.3.2.4 Group Activity

Again, as the study had to rely purely on the altruism of its subjects for co-operation, the selection of group activities such as a focus group or multiple-interview case study represented a considerable resource challenge. Even dyadic interviews were considered challenging; while a security manager may sanction a single hour of their own time, to commit several person-hours' resource to such a session was unlikely to be justifiable to management. This method would therefore have required the demonstration of a very clear benefit to be considered in a business environment.

Online forums (suggested by Flick 2009, p.269) were considered more practical than in-person focus groups since the subjects would be participating in their own time. Since the human interaction would be reduced, which is the key differentiator of the method, problems of arranging access across multiple subjects simultaneously were not felt to be outweighed by the minor benefit of allowing the participants to compare their own experiences directly.

4.4 Data Gathering Summary

Bringing together the theory, practical and methodological aspects from above, the choice of data gathering method is presented below.

4.4.1 Initial Selection

A filtering step was first applied to identify those methods which were still considered to be both applicable and practical, after which they were considered in more detail. For expediency, the methods are summarised as Table 3 below giving a short discussion of each.

Method	Challenges
Single Case Study, Ethnography	Rejected. The exposure to the risk of a single late withdrawal was unacceptable and this approach might not have provided sufficient data, particularly on the historical and regulatory perspectives.
Multiple Case Studies	Rejected. This approach would have required co-operation from multiple internal sources on a sensitive subject, some of whom would be at a senior level, thus the risk of not gaining sufficient access to data was not acceptable.
Focussed Interview	Not preferred. No suitable focussing device was identified and the method was not considered to have any characteristic making it especially suitable.
Unstructured Interview	Not preferred. It was likely that analysis would wish to compare differing answers on the same topic.
Semi-Structured Interview	Considered. See below.
Expert Interview	Considered. See below.
Problem-Centred Interview	Not preferred. This method is aimed principally at researching social problems and had no particular advantage to justify the additional complexity.
Narrative Interview	Considered. See below.
Dyadic Interview, Focus Groups	Not preferred due to the access challenges of reliably obtaining similar joint resources in a sufficient number of companies, relative to the limited additional insights gained.
Media Analysis	Considered. See below.

Table 3: A summary of candidate methods following the initial filter.

4.4.2 Media Analysis Trial Study

Data was sought for a historical account of the formation of a candidate profession of IT Security. An early strategy for the collection of this historical data was to search the archives of the security or general IT press, to attempt to observe any split from an IT parent profession

being reflected in contemporary reports. A numerical count of security-related positions advertised would also represent an interesting minor addition to the account, indicating how and when the security roles developed.

A trial study was undertaken by reviewing articles from the “Computer Weekly” newspaper, available in physical archive at the British Library covering 1966 to 2011, when it moved online. A preliminary perusal of around one hundred and twenty issues was conducted, selected at random. A trial coding frame was constructed using the procedures of Qualitative Content Analysis (QCA). QCA was chosen for two reasons: firstly its ability to reduce large amounts of data quickly given the scale of the data available, and secondly as the material could not be easily removed from the archive and could not practically be copied, coding needed to be possible directly from source.

It became clear that where security-related articles were examined, these were reported, not unreasonably, as fact rather than the nexus of a set of opinions in an unresolved controversy. It was felt that while interpretation could possibly characterise contemporary attitudes during analysis, this would be at the risk of “over analysis”, requiring substantial amounts of inference to establish how a network had been constructed.

Another avenue considered was to triangulate events reported with the interview data, which has some precedent. Chun and Mooney (2009) studied the emergence of the Chief Technology Officer using a triangulation approach, as they found this was the only way to achieve publication (M. Chun 3.3.2012, *pers. comm.*). In the trial however it was found that constructing a coding frame which could encompass almost any computer-related topic from four decades’ editions was difficult and a useful output impossible. The trial was therefore abandoned.

4.4.3 Discussion

The research questions comprise three elements: origin, status and direction. Three potential sets of actors are already visible: the people who wish to professionalise security, practitioners who may or may not wish to be professionalised, and government which may or may not wish to grant jurisdiction. At the outset it was proposed to limit the study to these sources to delineate the account according to the arbitrary property of the resources available (Latour 2005, p.148). Further groups could then be added (as was indeed the case, as described later) should the data collected direct this whilst “following the actor”.

It was resolved to gather data in each of these three areas, each class being expected to bring a different perspective. The practitioner would advise which factors have led to the creation of

their role, as well as discussing their status as they perceived it during their working lives. Those who work in professional associations were expected to have more considered views on the professionalisation topic and could provide experience of that process, possibly including some historical details. Those in government would not necessarily have had a direct interest in the origins of the profession unless personally involved by chance, however they are experts in current policy and the factors which had caused any recent movement in the area. Therefore all three groups have valid information to contribute to all areas and each has an active part in shaping the future. Semi-structured interviews were selected, to strike a balance between imposing structure onto the respondent's answer and a weakened analysis based on heterogeneous and incommensurable texts.

4.5 Data Analysis and Coding

Having identified that data would be gathered by interview, a method which generates a substantial amount of transcribed text, it was necessary to select a method of analysis, which almost inevitably for qualitative work involves *coding* the data.

4.5.1 Coding Methods

The analysis of data by assignment of one or more codes is an extremely popular choice for qualitative analysis (Bernard 2000, p.443) and can be used either to merely organise and reduce data or to question it, revealing new concepts (Schreier 2012, p.38). The codes applied can be determined in advance from other sources (possibly working hypotheses drawn from other research) and used deductively for confirmation (Bernard 2000, p.444) or as far as possible generated objectively from the data such as with Grounded Theory (Glaser and Strauss, 1967).

In reality it is accepted as impossible to exclude completely all pre-existing attitudes and theories (Gibbs 2007, pp.42–46), however the lack of a formal requirement for pre-existing codes can be useful where there is no accepted applicable theory (Orlikowski, 1993). Since there had been little work published at the point both of design and analysis (Burley *et al.*'s work for example not being published until (2014) and in any case taking a very different theoretical approach), an exploratory approach was appropriate. Whilst there is a large range of possible coding techniques (see Saldaña (2009) for a concise discussion of the field), perhaps the best-known and most widely used are Grounded Theory and the various forms of Content Analysis.

Grounded Theory discovery is a reaction to what its developers saw as the contemporary prevailing thesis of sociological method. Rather than rigorously verifying hypotheses theorised

elsewhere, the analysis of data can itself generate theory grounded in that data (Glaser and Strauss 1967, p.1). The induction versus deduction directionality (from the data comes theory) is held by this school to be paramount, to avoid *examplifying*, or the confirmation of a theory which was actually previously held with a conveniently selected empirical datum (Glaser and Strauss 1967, pp.5–6). The authors therefore argue that it is not simply a method for organising data (pp.132–133) or justifying hypotheses which originated elsewhere. The attempts to verify such hypotheses pollute the process of grounding theory in the data and then constantly comparing new data to that theory.

Qualitative Content Analysis (QCA) is a systematic but flexible approach for exposing meaning from within text (Schreier 2012, pp.1–19). There is in some cases a strong emphasis on validity, ideally through double coding (coding being performed by more than one researcher) or re-coding after an interval. It differs from standard coding methods as its intention is to reduce data volumes by examining it from one distinct angle after the creation of a coding frame and summarising the data through the coding. To achieve this, codes are mutually exclusive, in that the target text is split into sections and each section assigned one code only, differing from the multiple codes and highly reflexive coding processes used in other techniques such as Grounded Theory coding. (Schreier 2012, pp.37–57).

Content Analysis can be used in a positivist epistemology to verify a hypothesis but this is more usually associated with the quantitative form (hence this is not considered in detail here); QCA is also compatible with an interpretive ontology and an anti-positivist epistemology, requiring the reader to interpret the text to understand the viewpoint of the source (Graneheim and Lundman, 2004), although it is also deployed alongside quantisation and subsequent statistical analysis in mixed-methods studies (Sandelowski *et al.*, 2009) and can also be used by those taking a realist ontology (Schreier 2012, p.47). As discussed above, this study takes a more interpretative approach which does not well support positivist or realist concepts, thus the flavour of QCA considered here would be its more usual role as interpreting, summarising and describing data. In this way the movements of actors over a long period should be visible.

4.5.2 Selection

Both forms of textual coding described above would be valid choices and are well-accepted for analysing fieldwork. Grounded Theory emphasises systemic abstraction and generation of theory from the text; QCA reduces and describes the text but shows less emphasis on the systematisation of theory generation. Although Grounded Theory is associated with a well-respected method of coding (and that is not challenged here), the suggestion that by rigorous and systemic means the subjectivity of human analysis can be effectively mitigated is not

compatible with the interpretative position of this study. Similarly with a single researcher study it would be difficult to achieve such reproducibility and validity even if it were wished due to the necessarily consistent bias of the researcher. Moreover, the preparation of an ANT account is *inescapably* subjective, given that it is the re-telling by the researcher what they consider to be the pivotal events from stories heard from the subjects. No undue emphasis is therefore placed here on achieving objectivity and reliability through coding processes. Of greater importance was the construction of a frame to bring order and coherence to as many nuanced codes as could be practically supported without losing the ability to identify some common concepts or frequent assertions in the text.

Those techniques which are interested *principally* in applying codes in an entirely reproducible way – if necessary at the cost of capturing nuance – such that the truth therein can be captured free of interference from subjectivity, are not useful for this purpose. ANT itself is a sensitising guide for the researcher and has been suggested as a way to generate theory well-grounded in the text (Whittle and Spicer, 2008). It is perhaps possible to become *too* fixated on technique at the expense of achieving an interesting and broad account for debate. In constructing a coding approach, the fundamentals of Schreier's approach to coding and analysis were seen as *marginally* more compatible with the study's ontology due to the higher flexibility and lower emphasis on systematisation (although it too emphasises validity more than is considered useful here). The necessity to code the entire text was seen to be beneficial in ensuring that the researcher was forced to consider the full data set, rather than those parts which appeared significant during the analysis, in case something not previously identified as salient is accidentally missed. As Saldaña (2009, p.15) warns, this is a particular risk for less experienced researchers.

In this approach there is no theoretical limit on the number of levels or sub-categories allowed, however it is suggested that human coders are not practically able to cope with more than around forty such units in total. This limit may of course reflect an emphasis on validity and thus achieving high inter-coding Kappa values rather than achieving the widest possible range of captured concepts. Given that this study is interested in multiple related but not completely atomic concepts, to attempt to fit all data into such a narrow frame for exploratory work was considered impractical. In Schreier's (2012) text it is proposed that categories might represent *dimensions*, where the data is examined in terms of *each* category. Sub-categories must be mutually exclusive (data matches only one category) and exhaustive (data can be accurately coded by a category). That is not seen as useful here (since data answering a discrete professionalisation section is unlikely to be usefully also coded into a history of security section), therefore a more straightforward hierarchical but single dimension frame is preferred.

With respect to frame construction, Schreier's "hybrid" model was preferred, where an existing understanding of the subject area is used to create a conceptual frame (to seed the analysis and to show whether any of the underlying assumptions are not found in the data) but to extend this where the conceptual model is found wanting. Since the research questions identified discrete themes these were felt to be useful in allowing an entry-point for coding.

Some departure from Schreier's model was desired however, since in her (2012) model a coding frame is first established from around one tenth of the data, finalised and then applied to the rest of the material. That is explicitly rejected here, since this seems to imply that the coding is so general or the data so homogenous that a sample of the data contains everything which can be usefully learned concerning the frame. In this study it was determined that the frame should be developed as each additional text was added and analysed, with codes condensed either due to near-duplication or undesirable proliferation, thus allowing for being "surprised" by the data. This brings the method closer to the General Inductive Approach (Thomas, 2006).

Given the volume of data expected to be analysed and coded, as is now common it was considered most efficient to make use of computer aids for coding and analysis, commonly termed Computer Aided Qualitative Data Analysis Software, or CAQDAS.

4.5.3 Units of Analysis

Coding is performed on three types of segment: units of analysis, coding and context. Choosing a unit of analysis in this case is straightforward, since as an interview represents an easily-identified single, internally related text. Units of coding (or "units of meaning") represent the block of text which is atomic (in other words which is assigned to a particular subcategory without further dissection), which varies between dimensions according to the information required. It comprises those sections of text which are "related to each other through their content and context" (Graneheim and Lundman, 2003). Whilst considerable debate can be had on the topic, this study is aligned with the assertion that "Social interaction does not occur in neat, isolated units" (Glesne, 2006 cited in Saldaña 2009, p.16), and suggests that to analyse in more regulated units is to deny the possibility of multiply-nuanced short passages of text in favour of achieving higher rates of reproducible but narrow coding. By choosing a variable length unit of coding, clearly the unit of context (that part of the text needed to understand the unit of coding) becomes similarly variable and this is discussed in the report of the work as performed.

4.6 Research Plan at Outset

The original research plan was as follows:

A series of semi-structured interviews will be undertaken with security practitioners. These interviews will include a narrative section designed to elicit the respondent's view of the creation of their own role and the events which contributed to the formation and separation of a profession if they consider this to exist. They will also contain elements reflecting their perceived status in their role relative to other "benchmark" professions and their opinions concerning the professionalisation of the industry. Further interviews will be undertaken with professional associations in the IT Security sector, following similar topics using an instrument which reflects their expert status and which queries the direction and aims of their organisation with respect to professionalisation. Interviews will also be sought with government to capture (in addition to the general themes noted above) the perspective of the state with respect to the desirability and progress of the professionalisation of the security sector and delegation of regulation to a professional body. These interviews will be recorded (where the respondent agrees), transcribed verbatim and analysed by Qualitative Data Analysis using suitable software.

4.7 Execution of Research Plan

The research plan was executed first by fieldwork between September 2012 and February 2015, including an initial pilot phase of three practitioner interviews conducted between September and November 2012. In the following sections the practical details and developments to the project which occurred during this period are described.

4.7.1 Instruments

Two sets of instruments were created and submitted to the University ethical research process along with a research design and ethics statement, alongside details of how the data would be processed. The instruments as used are reproduced in Appendix 1; the following sections detail their creation and the ethical considerations involved.

4.7.1.1 "Notes for Participants"

A double-sided sheet was supplied to participants prior to the interview stating the purposes of the research, the background and identity of the student, the right to withdraw, the intended processing of the information and the uses to which it would be put, a signed copy of which was

kept to ensure a record of informed consent⁶. The document was prepared for the practitioner class of interviewee (for which amendments to data processing statements were required by the University) and then adapted for other classes as appropriate (reproduced in Appendix 1).

4.7.1.2 Interview Protocol

A semi-structured interview protocol was prepared from topics identified during the construction of the research question commentary given in the literature review chapter, after reviewing multiple qualitative research and interview technique resources, particularly Foddy (1993). This was again adapted for each class of interviewee according to the information sought and the emphases of each type of interview, along with modifications made to incorporate information learned during the pilot phase (see below). The protocols are also reproduced in Appendix 1.

4.7.2 Ethical Considerations

The principal ethical concerns and their mitigations as originally identified were:

- Ensuring informed, positive consent.
 - Full disclosure of the research aims and the storage and use of the data were explained in the signed “notes” document.
 - Right to withdraw and freedom not to participate were drawn particularly to the interviewee’s attention.
- Anonymity. Whilst interviews would not by design require discussion of security-specific information, it was possible that some sensitive information may be divulged either because it was germane or as background to a general discussion or anecdote.
 - Interview transcripts were originally to be *completely* sanitised (that is to say with all potentially identifying information removed) and anonymised fully, referenced only with a non-identifying demographics tag, with the original recording deleted after accuracy verification.
 - Quite correctly the University reviewers suggested this would make it impossible to identify and remove the contribution of a particular participant

⁶ For one telephone interview a copy was undertaken to be sent but was not received despite several requests. Verbal consent was gained immediately before the interview.

should they have chosen to withdraw. This was therefore changed to include an interview-specific code (see Appendix 3) but for this information to be linked to the identity of the participant only in a separate file stored elsewhere, which would only be accessed when necessary.

- It was further suggested that the analysis could not practically be restarted should a participant withdraw, thus the notes were updated to state that contributions which had already been combined with others to form conclusions could not be guaranteed to be removed.
 - Similarly it was planned to delete recordings of interviews, which would have made later examination of the transcription process impossible, thus this was changed to storage in encrypted format.
 - For the Central Government interviewee, given the almost unique nature of the interviewee's role and hence far greater likelihood of their identity being deduced, it was particularly drawn to the interviewee's attention that identification was a serious possibility. The interviewee was relaxed on this point since it is *part of their paid role* to speak on the record on the topic on behalf of government. The potential identification risk was therefore very effectively mitigated by the interviewee's own terms of reference and considerable experience as a public official.
- English Language
 - Participants whose first language was not English were offered the opportunity to request slower speech or bring a translator.
 - Potential for conflict of interest between the interviewer's employment and the position of the interviewee (for example if the interviewee's employer was a customer or supplier of the interviewer's employer or if they were colleagues).
 - Cases where respective employers would create a conflict would be avoided where known and the notes asked the interviewee to bring this to the attention of the interviewer if they were aware of such a conflict. In one example case the situation was discussed prior to interview and it was determined after investigation that the two companies were not direct commercial rivals.

- The case of the interviewee being a colleague of the interviewer was mitigated purely by reference to the nature and type of interviewee sought, who would always be hierarchically superior to the interviewer and hence very unlikely to suffer any power imbalance.
- The notes reflected that the interviewer was acting in their personal capacity, even if their professional identity had been somehow disclosed. This was important as the student's professional level of national clearance was felt to be an advantage in establishing *bona fides*.
- Protection of non-relevant personal characteristic data, such as gender, race and like matters.
 - These factors were not felt to be relevant to the specific research questions and hence were not included in the questioning. Wording around an undertaking not to record such details was changed however, as again the reviewers helpfully noted that where the interviewee offered this information *spontaneously* in the text it would be near-impossible *not* to record it during transcription even if it were not actually processed in the analysis. The element of "no intent" was therefore added.

4.7.3 Pilot

A pilot study of three interviews was conducted between September and November 2012. Two participants were recruited through contacts from the student's own career, however neither participant had themselves at the time of interview worked with nor had any personal connection with the student. The third was contacted following a request to the Hertfordshire branch of the British Computer Society (BCS). All three readily agreed to participate. The pilot data underwent initial analysis for inclusion in an interim report to justify undertaking further research at doctoral level, which was submitted in December 2012.

Aside from the above, the purpose of the pilot was to validate the methodology, research plan and instruments. The readiness of the interviewees to participate was highly positive given the risk of poor access to data to which the project was exposed. In addition, there was no resistance to voice recording nor hesitancy in accepting the confidentiality statement thus validating that aspect of the research design and assumptions.

Aside from minor changes to question ordering and format to reflect the natural course of

conversations as observed, the following changes were made to the practitioner protocol following the pilot:

- Interviewee's Biography: Themes of professionalisation, credentialing and education were rich sources of data. Whilst the narrative questions (describing personal career and the origin of the interviewee's role) were successful in producing a substantial amount of text, much of this was centred on career history which was much less directly relevant and these two questions often overlapped. In the next iteration of the protocol this aspect was down-played significantly. In addition, interviewees' interest visibly waned after around 75 minutes thus the overall time required was reduced.
- Interviewer's Biography: The original protocol included a very short explanation of the interviewer's own biography. This was later seen to be both unnecessary and potentially could change the answers of the interviewee if it changed the perception of the interviewer's knowledge of the area, thus was removed.
- Role Creation: More emphasis was made on drawing out the factors which led to the creation of roles or the expansion of security. These had varied considerably between respondents, often on industry lines. From the first interviews this naturally seemed to flow out of the career history section, particularly where the interviewee had longer experience as they had overseen or been part of that expansion. As a result, these questions were merged.
- Mandatory Registration: Specific questioning was introduced about whether the interviewee supported a mandatory registration scheme and whether qualifications were seen as essential. Qualifications bodies have been identified as a possible actor attempting to represent the industry, so this questioning was designed to see whether the participant was aligned with this. Specific questions concerning hiring a CISO without a qualification were introduced to determine whether these were seen as *de facto* barriers to entry. More emphasis was placed on whether IT Security was seen as having an ideal career path (degree, pre-registration, experience, professional qualification and so on), similar to more established professions. Previously, in error, it had been assumed that there was such an ideal path however this was not seen in the early data.
- Polysemy of "Profession": In the question "What does 'professional' mean to you?" the word "professional" was replaced with "profession". The former term was frequently not interpreted by the interviewee as was intended, viz. to stimulate debate on the class of occupation, something which could not be corrected without seeding their answer.

- User Education: The question concerning user education was re-worded as it was felt in retrospect to be in danger of "guiding" the interviewee to an expected answer and emphasis.
- Security Responsibility: It was felt useful to explore whether security has lobbied to be treated as a business priority at board level and whether this was genuinely lived, following early interesting answers.
- Leverage from Media Events and Incidents: Specific questioning was introduced following suggestions that this might be a possible mechanism of exerting influence.
- Termination: Switching off the recording was delayed as it was found that the interviewee occasionally wished to stress something said earlier.

The changes to the protocol were not considered sufficient to warrant excluding the answers gathered during the pilot from inclusion in the project's overall data-set, since they were of emphasis and organisation rather than of substance.

4.7.4 Main Phase Recruitment and Demographics

For the main phase, "practitioner" interviewee recruitment was initially through direct mail application addressed by job title to a list of organisations. Approaches were made in four tranches to one hundred companies, selected from the FTSE250 to provide access to the UK large enterprise sector. Selection was on practical grounds of head office location and where possible to a variety of sectors. Due to the breadth of roles related to a classical definition of security as noted in Chapter 2, hard criteria for further participant selection could not be justified theoretically. It was considered that a wide range of participant viewpoints could usefully contribute to the study. Similarly as no statistical treatment of quantitative data was proposed which would have required correction for identifiable variables, it was preferred for participants to self-identify as having a job role relevant to the topic of research. Had a respondent volunteered whose role did not appear to include responsibility for securing an organisation's data then these would have been declined. This eventuality fortunately did not occur and all offers of participation were able to be used.

Invitation letters were addressed to "The Chief Information Security Officer"; whilst not every organisation was expected to employ a person with this exact title, it was expected that the most suitable person would be identified through internal mechanisms and ideally answered or delegated to another person considered relevant upon receipt. The letter explained the purpose

of the research and requested participation from the recipient or a member of their team. Five interviews were produced from these approaches. It was made clear in the initial approach letter that the scope was limited to the personal history and attitudes of the interviewee, rather than formally representing the position of their employer. This was assumed to be a less threatening prospect in terms of revealing data and more appealing in terms of subject interest, as well as requiring only that individual's time without expecting them to expend their own energy to secure time or clearance from others.

Even so, as recruitment relied heavily on altruism, a degree of volunteer selection bias must be acknowledged. As altruism and alignment with the profession rather than the role are indicators for professionalisation, it is assumed that those willing to assist with an academic study are likely to be those most open to the prospect. It was not possible to exclude this bias from the study.

Following the initial approach by letter, an additional vector was found by leaving invitations at a security conference with the permission of the organisers. The target audience of the conference was expected to be management and senior technical staff in the security and assurance communities. Invitations were addressed to all delegates, again allowing participants to self-identify as having relevant employment roles. This produced a far higher rate of return and was responsible for securing around two thirds of the interviews. A former colleague of the author was also recruited to provide access to smaller organisations as an approach to local SME-type organisations in the student's local area was fruitless. Industry type and size have been suggested as factors in security outcomes (Chang and Ho, 2006) therefore some variation in this area was desired.

It became clear during the interviews that the formation at university, already seen as a strong theme in the literature, would be an extremely interesting additional source of information, therefore permission was gained to add university security-related degree course leaders to the types of interviewee and tailored instruments were created. Approaches were made to almost all UK institutions offering security-related degrees within practical travelling range but with a view to avoiding academics who might be requested to examine the work produced. Response rates were low and the five such interviews represented all the offers received.

In total 27 interviewees were recruited with no withdrawals post-interview. These comprised practitioners (18), course leaders and lecturers from UK universities (5), senior figures in credentialing bodies (3) and one representative of HM Government with overall internal responsibility for the Information Security profession. An anonymised list of the final participants according to industry type, participant type and company size is reproduced in

4.7.5 Interview Execution

Interviews took place at or near the participant's place of work in all but two cases, which were conducted by telephone. An attempt was made to follow Foddy's (1993, p.21) advice that the interviewee should understand the origin of the question, to establish a shared situational basis for the interaction. His argument was that if the interviewer does not give sufficient context for the question the interviewee will inevitably attempt to infer it, preventing the formation of a mutually held frame of reference. Pre-empting and signposting of questions of professionalisation were therefore avoided where possible during the interview. As recommended by Drever (2003, p.24), prompts were used to clarify or re-phrase questions, with a set of probes prepared on the protocol document to ensure that answers covered the main points required. Interviews lasted between 60 and 90 minutes. The main area of variation was the length of the narrative element.

4.7.6 Transcription

The transcription protocol is reproduced in Appendix 4. NCH ExpressScribe v.5.6.3 audio playback software was used to aid the transcription however no speech recognition system was used with all typing performed manually by the student. Following Flick (2009, p.300), speech was transcribed verbatim, however as the exchange was seen as a “medium” and not the focus of the research, non-words and aborted sentences where no substantial content had been forthcoming were deleted. Continuous text flow which contained multiple independent thoughts linked by conjunctions were divided as faithfully as possible into individual sentences for clarity. Despite some interviews taking place (at the request of the interviewee) in public catering spaces with consequent levels of background noise, very little text was lost to being indistinct or overlapped. Almost all of the latter was question clarification where the interviewee suddenly comprehended the question and answered quickly. Completed transcripts were mailed to interviewees to reduce the risk of error, prior to including the data to be analysed. A very few corrections were requested, which were duly made, and a similar number of positive confirmation messages were received. In the main, however, no response was made by the interviewee and this was taken to be that no changes were requested (as had been stated). In the case of the Central Government interviewee, because this was taken to be almost “on-record”, it was ensured that a positive message of consent *was* received prior to including the text in the database.

4.7.7 Coding and Analysis Process

As discussed above, coding of transcripts took place using Qualitative Content Analysis (principally following the methods of Schreier (2012)). NVivo v.10, the standard tool recommended and used by the University, was used to facilitate this coding process.

The unit of analysis was chosen to be one interview and the context unit of an answer/question block. No obvious regular unit of segmentation was seen (since sentence structure was coder-imposed during the transcription process and multiple themes could be introduced within one short block), thus codes were assigned to phrases or blocks of text and these blocks separated in NVivo using carriage returns. Each block was assigned a code, which was either substantive (true data) or procedural (question, “social” conversation, clarification or off-topic).

Each interview’s data was added to the database immediately after transcription, however one interview at a time was coded in its entirety prior to the next unit being coded. It was not possible nor particularly intended to directly link categories to specific interview questions (see Schreier 2012, p.79), as it was found that (catalysed by the semi-structured format) interviewees

spontaneously introduced and interweaved many of the topics selected for discussion. Seed categories were therefore created that followed particular research question themes, however these were purely used as an entry and were regularly re-visited, expanded or condensed as the analysis continued.

As data was coded, a commentary “memo” track was maintained in NVivo separately from the textual sources where comments, practical notes (concerning mainly creation, deletion and combination of codes) and concepts identified were stored. From this it was identified that a new type of interview (educator) would be helpful. During coding, additional codes were created only when this could be justified to avoid an unmanageable frame, and rationalised where codes appeared to be both too infrequently used to be justified and their low use was not in itself considered to be particularly instructive. Clearly, as new types of interview were added new codes tended to be generated more frequently, both because the questions were specific to the type but also because the different contexts often brought changes in perspective and priority. Codes were gathered into major and minor categories in a three-level hierarchy, which was a highly iterative process since in reality some early categorisations were unsuccessful in establishing unique dimensions of thought and needed to be adjusted.

As with all such endeavours the frame represented the “best fit” distribution of general concepts across the major organising labels. A very widely-applied code for example was “Professional means...”, which was originally intended as a placeholder for problematic sections which proved difficult to code atomically. The attempt to break this data down into smaller codes however was somewhat unsuccessful. Due to the success of the “list of traits” model of professional status, most answers simply listed these traits, or very similar but nuanced variations on similar themes, to the point that individually coding traits would have left the text scattered as blocks of a few words over potentially dozens of individual codes. As the intent of the research is to look at the effect of the professional model and its homogeneity or otherwise across actors, this would have been unhelpful as there would have been few ways to truly see the notions of professional status side-by-side for comparison. Instead, the widely-applied code was left, then memos taken from an analysis of the text so coded, forming the basis of the following analysis.

Following the coding of all interviews, a further pass was made of all the data (the frame by this point having been established and stabilised) to ensure that data which had been coded in some cases over a year apart were reasonably consistent and to identify whether any further rationalisation could usefully be done. Further memos were added during this process. The first cycle analysis was then undertaken, where for each sub-category the data assigned to that category was read through and summarised, and combined with the memos relating to that data

to form an initial analysis organised by major frame category and then sub-category. The data for each category was biased towards the codes which had been seen (mainly by coding frequency but also by perceived theoretical significance) to be the most significant for the discussion. During this process additional memos were created and a working narrative constructed from the more abstracted notes taken in the earlier stages. The first stage analysis is reported in the next chapter.

A second-stage analysis was then made using the narrative and memos created during the previous work, whereby the major novel and unexpected contributions to knowledge were identified and grouped according to some overall themes. This allowed the tying together of elements from amongst the various branches of the frame into unified areas of theory, which were then argued and summarised in conclusions. This forms the basis for the secondary analysis in Chapter 6. The principal conclusions of the secondary analysis are then summarised and re-stated in the final chapter in juxtaposition to the original research questions.

Chapter 5: Conceptual Analysis

The analysis is presented in two stages. In this chapter, the data is summarised broadly according to theme and category, noting any contrasting positions of the participant groups. Text seen during the memo-writing process to be of particular relevance is highlighted, sensitised by the principal concepts of Actor–Network Theory: references are made to individual actors' visible traces rather than describing mechanisms with predictable patterns at the macro scale. This provides the foundation for the later secondary analysis.

5.1 Introduction

As an ANT account describes a network in the form of a web of interactions, that network defies easy reduction to a linear narrative. Indeed the linearity presented in other accounts is one of the criticisms made of macro-level sociology by ANT's proponents. To bring some structure to the interpreted data, the over-arching themes and their constituent categories (identified during coding and analysis) were also used to organise the discussion presented in this chapter. In addition to a housekeeping section, these themes were:

- Personal Aspects (the biography and career histories of the participants),
- Certifications (including a comparison of “professional” and academic certification),
- Professionalism (examining the profession *qua* profession), and
- Work Context (the practice of the profession within the enterprise).

After a brief review of the housekeeping text for completeness, each major theme is introduced and its significant data summarised in turn.

5.2 Housekeeping and Interview Administration

Six codes were created for topics which concerned the execution of the interview itself, rather than its substance:

- Question: interrogative statements intended to produce a response on a new issue, even if only a minor progression of topic, rather than to clarify a previous exchange.
- Clarification: statements used to gain more precision or address ambiguity relating to a question.
- Conversation: exchanges and comments which were auxiliary to the main questions or off-topic.
- Housekeeping: text related to the actual conduct of the interview, for example

interruptions, timekeeping and hospitality. Larger, contiguous sections were removed during transcription where possible.

- Not comprehended: text which did not appear to make grammatical sense and meaning could not be inferred from context, and so could not be coded.
- I don't know: the interviewee stated they could not answer a question and either refused or could not attempt to reply.

These codes were speculatively subdivided into “interviewer” and “interviewee” types where appropriate during coding, however in retrospect no use was found for this distinction.

One substantive code was included: “My thoughts on this subject are not fully formed.” This code was applied to text where the interviewee expressed the novelty of a topic, for example:

"I think it's really, really interesting what you're doing and the things I've come out with I haven't really thought about, to be honest."

[HEL42E-AN12]

After much thought, this was created and left as a general code rather than placed within one of the themes. Some of these codes were generated in tail-end conversation and wrap-up statements which would have separated them from similar text expressed during a formal question, thus losing the ability to compare them. Overall, eleven people stated outright that the topics of professionalisation and licensing were not ones which had been significant for them prior to the interview. In addition, memos taken during the transcription process note that several of the answers concerning these topics produced hesitant, less confident or less coherent remarks.

5.3 Personal Aspects

5.3.1 Overview

This theme concentrates on the interviewee as an individual, seeking the origins and context changes for practice as the interviewees recall their careers. The intention here is to observe actants shaping that context, identifying movements they may have caused— either directly or in actions they prompted in others. The theme is divided into two principal topics: Biography, the choices the participants made in their careers and how they relate to their roles, and Role Origin, how their current role came to be created.

5.3.2 Biography

From the literature it was theorised that participants would have seen substantial change during

their careers, and indeed for many Information Security practice would have emerged almost entirely within their working lives. As discussed in the Methodology chapter, the research design therefore adopted a part-biographical approach. This is now seen as an error in design. Whilst it fulfilled a minor aim of beginning with a comfortable topic which would relax the interviewee, the pilot study showed that by encouraging wide-ranging accounts of decades-long careers, a large amount of material was gathered which consumed coding and transcription time, without revealing evidence of any (interesting) actant.

It was determined that the interview protocol needed to focus more on the moment of change; what was in the mind of the interviewee at the time that security matters became of interest and what caused this change. The earliest four interviews prior to this change therefore comprise around two-fifths of the text coded as “Security-neutral explanation of work experiences”, where no useful evidence of enticement to join a network was seen. Similarly, a substantial amount of text was coded as “Description of responsibilities, achievements and structure in a specific security role”. This was applied to recollections where the interviewee had entered the security domain but where the text was of a general nature and did not appear to show useful evidence of actants at work.

The key role of this data is to signpost the disorganised and unintentional drift into security which is revealed later. The practitioner contributors were predominantly former IT workers, with two other voices: an auditor and a former secretary. Interestingly, the two non-IT-trained examples were both co-opted into Information Security sections for their advanced business and interpersonal skills. Only one (an outright technical analyst) had studied security pre-career with the intention of entering it, having been interested by the film *War Games*. After doctoral studies he joined his City consultancy employer and remains within their senior technical ranks. Similarly, the government representative trained as an engineer and when offered a choice of civil service careers was attracted to security more for salary reasons, being pragmatic on subject matter. In setting the context for the network, where “practitioner” is seen in its current context one should not assume the same degree of career intention, vocational training, socialisation and early alignment with peer groupings as is usually implied by “professional”. The black box of “professional status” in this network will come under scrutiny later.

All the academic interviewees started their careers in computer science; the alignment observed with Information Security as a *form of computing* within academia was very noticeable. One lecturer, whose career had developed after the third and fourth “waves” described by von Solms (2004), had found an interest in security very early on in his academic career and had moved positively towards it. The others, whose careers pre-dated this, had necessarily entered in mid-

career and attested to the lack of security focus in earlier computing research.

There was some commonality to the careers of the representatives of the professional bodies. All were well into the established phases of their career and with graduate-level engineering or computer science backgrounds. The move into security was more chance opportunity than intention in all cases, however passionate their later attachment. All were very knowledgeable about the foundation of their organisations, in two cases from direct personal involvement.

From the above it is seen that security as a topic developed during the careers of almost all the participants. In the following section the origins of their roles are explored.

5.3.3 Role Origin

The increased focus on security is relatively recent. Multiple attempts were made with the questioning to observe the causes of this change, both in general and the origin of the practitioners' own roles specifically. This was partly to provide an additional source of data – thought to be a relatively reliably-known matter relative more speculative recollections of history invited elsewhere – but also to explore individual incidents to avoid excessive generalisation concerning macro effects.

An unexpected insight was that some practitioners had personally agitated for increased security resources in organisations where it had not been a priority, noting the increased focus which had emerged externally and lobbying for greater internal emphasis.

“I was playing at being a team player and recognised that there was a bit that wasn't being done that needed to be done”

[MAN86E-DS66]

The management response in these cases was reluctantly to accept the need for change, but to delegate this back to the IT team. These agitators therefore reported gaining these additional responsibilities as a dubious “reward” for their efforts. This resonates with a code described later which notes where security is seen as a task to delegate rather than something to be owned by the board.

A potential network fragment emerges here. Boards need to ensure that “security is done”, which requires someone to whom the task can be entrusted whose judgement can be relied upon. Given the impact if unsuccessful, management requires a method either to guarantee their delegate is competent or – as some here mentioned – at least prove all due efforts were made, which discharges their personal responsibility. Some potential actants can be observed:

- managers who must delegate security-focussed work to a specialist,
- specialists to execute the task (a candidate *profession*),
- a device for those specialists to prove they are competent,
- a device for management to show due diligence, and
- a body to issue those devices.

This might be represented diagrammatically as in Fig. 11, using the key in Fig. 10. Throughout this chapter such diagrams will be used to illustrate the commentary in the text, identifying the principal actants, their interrelationships and the devices used to shape the network according to their interests. Such representations are of course only summaries, assisting simply by focussing attention on that part of the network under review. As networks are essentially unlimited and contain many potential alliances to examine, it is helpful to identify those fragments which appear most theoretically interesting, to help bound the discussion.

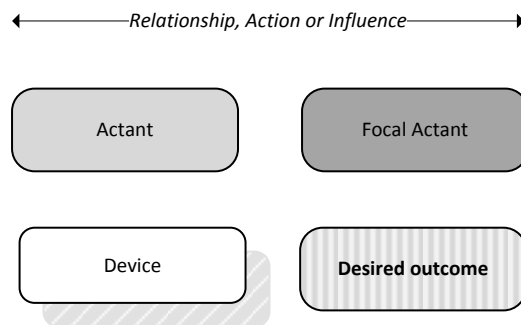


Fig. 10: Key to later network fragment representations.

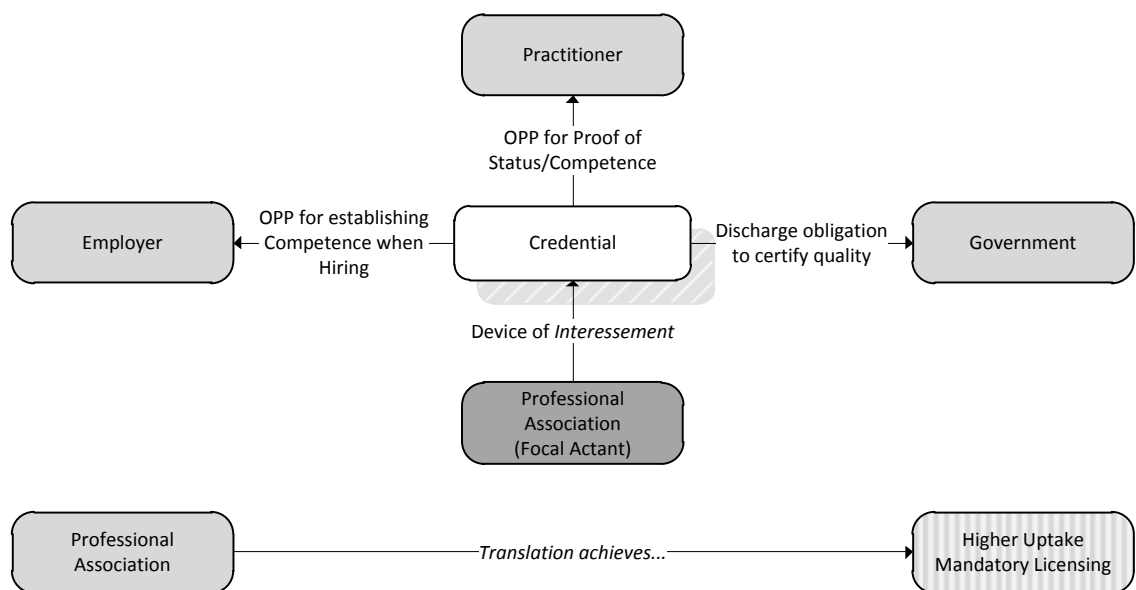


Fig. 11: Derived network fragment observed in the certification market.

This particular network will only become irreversible when security becomes complex enough to require delegation to certified specialists and a recognised device exists which is sufficiently in demand to be effectively *required* for practice. At this point it moves beyond a device of *interessement* to an *inscription*: an unquestioningly accepted artefact which can be used as currency. At this time it appears that the network is *not* irreversible end-to-end, in that the lobbying of management for control or resources is recurrent, thus accepting the advice of the specialist is not taken as mandatory.

“Unless you can get to the delivery stage of it, you're going to be forever fighting that battle. Communicating, getting an understanding, getting an agreement, getting some budget, doing it; you've got to get past to the ‘get the budget and do it’ and maintain.”

[MIN48E-SM22]

Similar stories were heard from the educationalists, who had to lobby for security to be introduced to courses rather than rely on external demand for degrees.

“At the same time, we weren't actually teaching any IT Security here, so what I did was I got some IT Security lectures included in some of the modules that I was teaching on at that point in time.”

[EDU45E-CL31]

Naturally the recollections of the interviewees will reflect their own achievements and concerns, and they may not easily be able to describe the genesis of a role pre-dating their time in the enterprise. The analysis cannot therefore rely too much into the “statistics” of the data. It can however be reasonably inferred that the actions of independently-motivated internal individuals were a strong factor in the introduction of security roles in some organisations. It is also seen that there was no obvious compelling external pressure beyond mimesis to introduce security into computing courses; developments here were similarly influenced by internals taking the initiative.

This is significant, because an ANT account must examine whether these practitioners are simply gears in a mechanism which translates some external event (such as the emergence of the I Love You virus) into internal action within an organisation (creation of a security role), possibly in the mimetic sense noted by DiMaggio and Powell (1983). Alternatively it might see these people as actors in their own right, potentially using some artefact which can be used – exactly as occurred above – as a device of *interessement*. This might strengthen a campaign to secure resources by being the OPP to protection from the vaguely-defined external threat the item represents. There is some minor material suggesting that at least initially the new practitioners had some leeway in their actions given by the novelty of the topic and the lack of precedence for management to follow. To consider this fully, this data must be seen together

with that reported later, where the practitioners talk down the prospect of using external actions as internal levers.

A number of the roles covered had rather vague origins, without a solid report indicating a fixed cause, particularly where the event was external but not specified.

“Yes, it came from the head of department basically saying, ‘I believe we need an IT Security role.’”

[CHA33M-SM54]

These cases show only that an increased security focus was somehow being generated and presume this was by the commercial environment but without a clear view on the cause from this data.

5.4 Certifications

5.4.1 Overview

As was noted in section 2.4.3, a number of certifications exist which may play differing roles in the network, or none. The data addressed in this section is mostly derived from questioning the interviewees' attitudes to certifications and attempting to detect what role these play in their worlds. The sections show firstly how academic certifications show similarities in *network structure* to their commercial equivalents but play a distinct role in a subtly different network, alongside considering how and why people are attracted to take each and what factors are in the mind of those who create them.

5.4.2 Academic Versus Professional Qualifications

Professionalism represents a monopoly of expertise over an area of deep, abstract knowledge. Many well-established professions are strongly associated with advanced academic learning; indeed the establishment of a degree programme is a key stage in the process described by Wilensky (1964). Whilst many comments discussed the role of “qualifications” as a general case, thereby creating a counter-argument for distinguishing between academic and professional qualifications at a coding level, this section looks mainly at academic education and where this is distinguished from qualifications in general. This is due partly to sensitisation from the literature review itself (suggesting that *pre-career* education is a success marker for a professionalisation campaign) and because the interviewee group included academic and professional certification providers allowing a contrast to be made.

Whilst the literature insists a professional claim must be to theory-based expertise, a strong case

was made – by all interviewee types but particularly practitioners – for distinguishing between learned theory, and practical experience and judgement, stressing the pre-eminence of the latter. The data suggested not just that additional soft skills are needed in the workplace, but that theory and practice may even conflict.

“When you're doing your ISACA exams ... you get questions which you've got to demonstrate a textbook response for, but actually in reality the question and the answer aren't what would happen in the real world.”

[FIN31E-AN72]

Although less common, there was even some scepticism shown towards those with qualifications.

“Theoretical qualifications ... aren't all that great because they've got very little to do with real life. I've seen a lot of people come through here with computer science degrees who haven't got a clue how to send an email.”

[TEC11S-ID48]

Whilst obviously feeling that their courses did prepare students for an entry-level position in the workforce, even the educators noted the importance of going on to gain experience.

“[Our students] all think they can walk out of this door and become a consultant. Now I worked for years before I went out as a consultant, and I still feel in every job that I've learned from the last one.”

[EDU24E-CL05]

The text in this section strongly questions whether possessing certificates is a guarantee of competence, deterring the enrolment of the practitioners and employers in the network described in Fig. 11. All of the professional bodies made particular reference to the requirement to have experience, which is significant since it marks a distinction between learned knowledge and taught facts, underlining the claim to professional status rather than simple examination success.

With two exceptions, who were both technical analysts, the clear feeling from the practitioners was that a specialist degree was not a necessary step for employment in the industry (some unaware even that such qualifications existed). Generally although not hostile towards them there was little enthusiasm for vocational security degrees. The educationalists were predictably far more positive about their worth, feeling that although they did not create the finished article they form a useful grounding of knowledge for a later career.

This is seen as highly significant as a negative finding seen against the professionalisation literature; if one were to contrast this with law lecturers and practising solicitors, a more powerful and harmonised statement of the almost essential nature of graduate pre-qualification

would surely be seen. Is this then a failure to professionalise, or a failure of the orthodox concept of professionalism in a modern profession?

The educationalist attitude is in line with the literature with respect to abstract knowledge. The conceptual nature of academic study – upon which the more transient knowledge of contemporary fashions can be overlaid using timeless principles – was strongly emphasised.

“I would prefer seeing a university degree [as] something that gives the ability to a student to adapt to any circumstances ... rather than making a graduate which is highly specialised but if you change something ... is completely useless.”

[EDU54E-CL11]

There is an interesting juxtaposition here with the distinction seen both in this data and in the literature between technical and social security concepts. Information about a particular state or moment in the development of technology was seen as a transient issue; by contrast “depth”, the principles of analysis and the underlying understanding behind the action, was seen as fundamental to the whole span of a career. Professional qualifications were seen as being far closer to tests of current knowledge and providing competent services, but without the intensity of contact time required to instil deep conceptual learning.

“Degree courses demonstrate ... an in-depth level of understanding and a demonstrable ability to analyse problems and apply new techniques and synthesise ideas. Accreditation does not do that. Accreditation demonstrates a broad understanding of a subject area.”

[EDU27E-CL05]

Interestingly there was little dissent from the professional groups, who were not interested in certifying abstract learning, rather attesting to well-maintained knowledge.

“A security master's is about understanding ... in reasonable depth security ... [Our credential] doesn't care about that, it just says, ‘Do you know at this level?’”

[PRO29E-PO42]

For those in mid-career, the prospect of undertaking a degree with its associated years of study is potentially impractical, with professional certification far more palatable. Thus from the standpoints of entry demographics, function and content, academic and professional qualification providers did not see themselves as in competition with each other, rather providing complementary products. Universities however did not see their role merely to teach the esoteric concepts of security theory but also to prepare students for employment and thus value industry speakers and even offer basic professional qualifications alongside their own courses. They are preparing a generation of students who have undertaken vocational courses with a view to employment who will gradually replace those who “migrated” from other disciplines.

In order for a course to be offered at a university (which educators reported must at least cover its own costs and should ideally generate income), sufficient student numbers must be enrolled. Students are attracted by the reputation of the university, which in turn translates to a more prestigious academic record. As competition increases, the fees chargeable by the more academically respected institutions can rise, particularly in the less regulated postgraduate market. Students in turn must justify the financial investment demanded, thus universities looking to enrol students must provide apparent guarantees of access to a career following the degree, thus employability statistics are highly relevant alongside the device of the degree certificate itself.

In turn, university departments (who reluctantly noted they must successfully market themselves to fee-payers) are approaching industry to assist in the design of degree courses to ensure employability and thus (through employment statistics) maintain an attractive credential. This is important, since a concern from the practitioners was how academic institutions divorced from day-to-day security work could maintain a relevant curriculum given the high rate of change in the subject matter. One answer given was for academics to undertake professional consultancy work in industry, providing an interesting blurring of the actors' identities in the network.

One educator reported a gap between their students' expectations – or perhaps their original impressions of security practice – and their experiences during the course.

“In the first year they have this concept of security as something fascinating, something joyful, but then they gradually start realising the seriousness of the situation.”

[EDU54E-CL11]

In terms of the network, although difficult without input from the students, it is necessary to attempt to see or predict the effect of this. Obviously it is important for the student and could even affect their choice of career afterwards, however university training is a socialisation process, therefore at the same time (according to orthodox models) they are being conditioned to align with the norms of the profession. Given this and the degree of investment into what is a relatively vocational qualification, it is predicted that the impression given pre-enrolment is the important one and subsequent change would be a less significant path to reversibility. The university is therefore initially an *apparent* passage point not simply to a career but an exciting role. Even if this impression changes during the course, the network's “potential student” actant has done its work; individuals transform into different actants over time as they become more experienced.

Within the course design elements, there is evidence of “security in its technical context” persisting. Whilst there was mention of the social aspects, on balance course content is

influenced by the technical background of the course lecturers amongst other factors. Given pressures of time and resourcing, each potential module must compete to win or keep its place in the curriculum. Each module can offer a passing grade to the student, thus there might be pragmatic or game-based reasons for their choices, however where choice was made available it appears that socially-informed courses are chosen at a reasonable rate and this will have an effect on the graduates produced.

It is possible to represent the network fragment described above diagrammatically, as in Fig. 12:

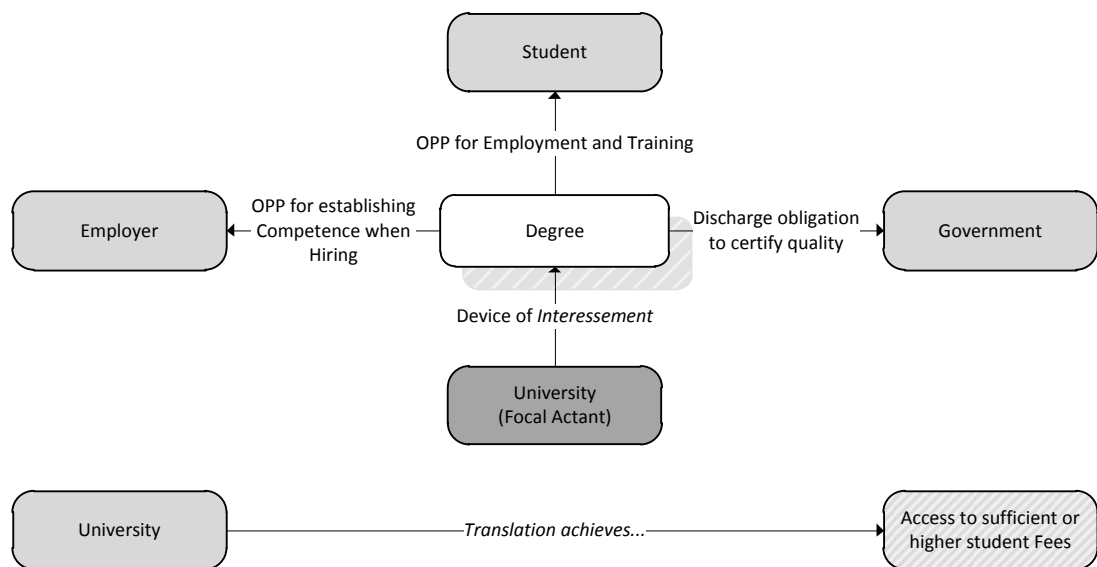


Fig. 12: Network fragment observed with respect to academic qualifications.

Whilst security courses are increasingly popular, universities have not yet established themselves as the sole passage point to a security career. The translation in Fig. 12 is therefore unstable and incomplete, since not only can the provider be displaced by other institutions (and subjects with greater potential reward and/or status), but the degree itself is not indispensable. This said, other factors are not represented: the student will have contemporaries, cultural inclination and predictable workplace competition which might make *graduate* status appealing, for which the class “University” *is* an OPP and for which they have finite financial and academic capital to buy from the market.

The data showed clear potential for change. Government action in answering industry’s call for more practitioners will surely increase the supply of graduates, potentially squeezing out those non-graduates who cannot compete on some other basis for entry; the degree device could therefore still be a powerful one. Universities certainly appeared to regard security careers as almost necessarily proceeding from graduate study, whereas neither government nor the practitioners are currently convinced. This may further undermine the unity of the role; government for example saw security as having too many constituent roles and too many levels

of practice to be an exclusively graduate profession, but acknowledged the positives of graduate study at master's level.

“Doesn't have to be [a graduate profession]. I mean, we run an apprenticeship scheme ... for people coming through. I think you have to have a certain aptitude and it depends what the particular job is as well, what the particular work is. Because there's different roles, different skill sets needed and some of those skill sets are very attuned to people who have come through more vocational education and training. So no.”

[GOV01E-GV01]

Government actions will act to modify the market, introducing through CESG approval processes for master's degrees in security (at the time of interview). Since security became a popular subject for study, alongside those with strong genuinely security-centred courses, others apparently relabelled existing programme modules as “security” to make them more marketable. Although surprising, this was confirmed by several sources, for example:

“I know of higher education institutions that will call something an IT Security degree when in fact it is the computer science degree with maybe one module of IT Security attached to it, which is not entirely desirable.”

[EDU45E-CL31]

Within the network, therefore, the status of any given degree programme as a pathway to a quality security graduate becomes suspect. Universities must assess whether the likely commercial benefit to taking the steps needed to obtain the “quality marker” badge can be justified against the cost of doing so. Internally the academics may wish to have confirmation of the quality of their course for prestige or professional pride, however in the financial reality of higher education, it is seen simply as a business opportunity.

“And so if it turned out that the cost of getting GCHQ certification was not justified by the perceived extra income that would result from it, then I think the department would not be interested in getting the certification.”

[EDU66E-CL71]

The network acted to push for a test of quality when government found itself being requested to recommend or certify the high-quality degrees from amongst the eighty-five then-available programmes. It therefore found itself with a role which it felt unable to discharge.

“As a government department I can't say, ‘Go to *that* university rather than *that* university,’ because I have to be fair. And at the end of the day, I don't actually *know* whether that course is any good. So what we did was we set out doing that certification with the aim that it will help people to navigate through the complicated world of the education that's out there.”

[GOV1E-GV01, emphasis added]

Seen against the professionalisation theses of authors such as Wilensky (1964), this is an opportunity to press for a professional body. The case for regulation of an area of knowledge has been made and accepted in this specific regard by government. Government needs to delegate

its by-default responsibility for national coordination, candidate bodies exist and yet the delegation of authority is to a panel; GCHQ retains the visible ownership of the badge which is awarded even though it does not directly assess the programmes.

The driving focal actor here is therefore seen to be the government (shown in Fig. 13), which according to historical models is unusual in the UK. This suggests a weak or ineffective campaign for control of knowledge by the relevant nascent profession.

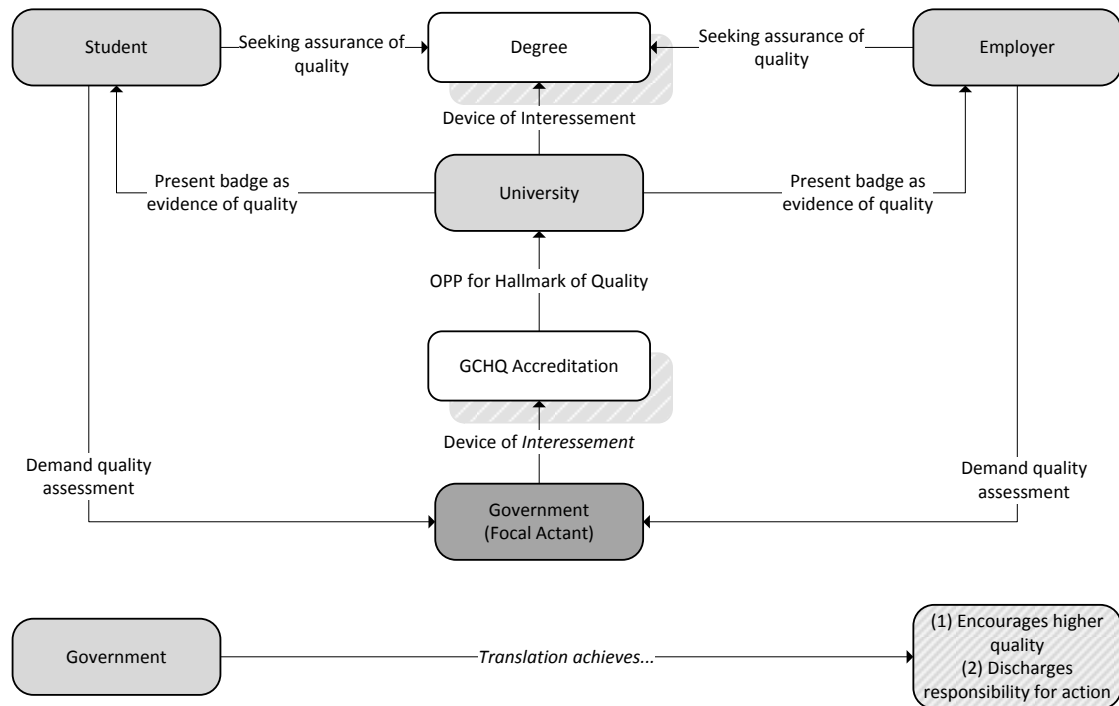


Fig. 13: Network fragment observed with relation to GCHQ accreditation of master's degrees.

The practitioners were cautious in their approach to university education, stressing the paramount importance of experience. Such people were however not themselves recruited from an academic background thus they are possibly suspicious of any mandatory graduate education for “competent” status (F. Piper, *pers. comm.*). This would either leave them unqualified for their own role or facing the considerable task of undertaking a degree alongside full-time employment to learn knowledge they would already claim mostly to have. Conversely they were themselves required to be pathfinders in a new field of practice, learning their trade from a variety of sources, thus naturally they would be expected to favour field experience over theoretical knowledge.

“I didn't have any qualifications when I came into the role, no specific security qualifications, you just had to have an aptitude, a willingness, an interest, and that seemed to be enough to inspire people to give me a chance for the role.”

[CHA31E-SM07]

This is a serious threat to the irreversibility of the *current* network, but the increased supply of

security graduates will necessarily change the make-up of those entering security. Since it was already seen that the current generation of managers and CISOs in large part were unable to follow this entry path, it is surely reasonable to expect these new vocational graduate entrants to go on to occupy senior roles to a greater degree than at present, where they will in turn appoint future entrants. These people will surely consider graduate training to be more useful and hence increase the effectiveness of the universities' degree device. In addition, it was acknowledged that graduates might have an advantage *ceteris paribus* over non-graduates as the wave of additional security graduates may address the current shortfall of talent; this may change the balance between hiring manager and entrant, thus generating more competition amongst entrants and favouring graduates.

5.4.3 Professional Qualifications and the Certifications Market

Professional credentials can be seen within a superficially very similar network to the academic degree, however their role can be understood very differently. The complementarity can be seen from the practice of some universities to encourage students to take basic practitioner technical examinations. This is not seen as competition to the degree's greater and more in-depth learning and helps to improve employability. As with degrees, credentials such as the CISSP or CISM are potential devices of *interessement* for their issuing bodies, however rather than being the basis for a claim to being worthy of employment at a basic level, these are the start of a claim to professional status and competence.

Such certifications are currently in a rather peculiar market. In one sense, it is beneficial for the network to solidify around a *de facto* requirement to possess a certification for practice. Without such a move there is an alternate path to employment (or *competent* status), with its own costs and benefits, which will be in perpetual competition with certification. The certification market might be able simply to agree some demarcation along a subject-matter or seniority axis and hence allow multiple certifications to co-exist. One might therefore expect an incentive for co-operation between the certifications to ensure that *one* of their set becomes mandatory and as a whole they become an OPP.

One provider however dismissed this, noting that certification schemes require substantial investment in advertising, with a questionable return if the advertising also benefits a rival. Providers therefore act to promote their product alone, even if in terms of game theory there might be better stratagems. Within the certification market itself, there would potentially be benefits to rationalisation. To become a true OPP, the market must coalesce discrete areas of knowledge into one qualification per specialist area, either through market forces or by regulatory action. Until that point the situation may be perfectly sustainable of course, but the

network will not be irreversible since it can be attacked by another established or up-and-coming credential with a greater perceived benefit to the enrolled actants. Once market dominance *is* established, that should be a platform from which to offer credentials as reasonably essential (albeit *de facto* not *de jure* through licensing).

So has market dominance been established? Put simply: no. The most widely-discussed credential by the practitioners was the CISSP from (ISC)², with CISM from ISACA also well-known, both being reasonably well respected. The CISSP is thus arguably closest to being the “default”; it is seen as a broad test of general security knowledge, and thus aside from the feat of actually surviving its six-hour examination, it is seen as neither being nor claiming to be a “single criterion” test of outright competence as a security practitioner. There was no real criticism to be found for it, purely that a single multiple-choice examination could not replace real field experience for proving competence, nor threaten academic study for depth.

There is an outright failure of the device to convince here. The CISSP has a substantial minimum criterion of five years’ experience in direct security work, with only one year waived if a degree is also held. It appears therefore that professional standing is reckoned to be acquired *overwhelmingly* through experience and currency of knowledge if only 20% can be substituted by prior very deep conceptual education. This qualification, then, exists to prove *competence* and thus become an OPP for professional status. It is strange however that this device of *interessement* so heavily based on prior experience should not successfully inscribe itself precisely because it can allegedly be bypassed *by having sufficient experience*. The danger of someone being able to practise incompetently for a long period of time and gain invalid experience was only mentioned sparingly.

Also mentioned, albeit more by the educators rather than the practitioners, was membership of the IISP. As noted in section 2.4.3, this organisation is evidence of a challenge to security as a computing-related subject. Ultimately the BCS – despite charter body status for IT and despite its commercial arm offering the government-backed qualification – has *not* become an OPP for professional status. Whether this is because the community feels security is best represented outside the computing realm, or purely because the British Computer Society (BCS) did not perform with sufficient energy and purpose is not clear. Both points of view were advanced.

“The IISP goes in deeper to the actual person, their characteristics and what they've done previously, where they are now and depending on the amount of experience, on what you understand and your practical knowledge they'll grade you, they don't just go, ‘Here you go, there's a badge, you're now in IISP’, it's not like that.”

[FIN91E-SM15]

Strangely, although the participant group was overwhelmingly from an IT background, the BCS was barely mentioned. Similarly the founders of the professional organisations were clearly from academic and industrial computing backgrounds, and yet chose to create new organisations. Whilst this is too insubstantial to be seen as “proof” of Abbot’s thesis of professional fracture, it is entirely in keeping with it. In this study of UK-based practitioners, there was a distinct antipathy (sometimes expressed off-record) towards the BCS which might explain the separate existence of the IISP.

A potential challenge to the latter’s success will be its single-nation element, when security is not itself a national challenge. Within the accounts of the practitioners and the literature, some traces of non-human agency can be seen in the globalisation and additional regulation of the industries who have the biggest resources to address security concerns. As such organisations operate in multiple jurisdictions, a credential which is respected in one territory may have no such cachet in another, reducing its lure for the potential candidate or its likelihood to becoming a required credential for the organisation. An internationally-recognised qualification such as the CISSP or CISA may therefore have a greater claim to giving status, which may act to limit any perceived loss of quality. Of course multiple certification is possible, however this requires extra resources and also erodes the sense (common to regulated professions) of a binary status of “qualified” or “not qualified”.

Furthermore, within the network it was very noticeable how data protection was used by many participants as the principal example of legislation which has forced Information Security issues into the boardroom, coercing action regardless of the organisation’s overall security posture. Risk management decisions are about selecting from the available options; for most organisations illegal non-compliance is not a genuine option. Even where the state-imposed punishment is relatively small, as was felt to be the case for example for Data Protection fines for a substantial multinational bank, avoiding the reputational damage from exposure as a compliance-evader was seen to be compelling.

As a byword for “regulatory mimetic pressure” this can be seen as an inscription in the network, hinting at where the security function’s policy has significant power. This black box however suffers little unpacking; as the practitioners made clear, different territories address this topic very differently. The potential CISO must therefore ensure they have access to the relevant topics in all operational districts, which in turn requires them to be aware of this international variance and hence moving the international dimension for certification up the list of candidate priorities.

Being internationally relevant similarly has an effect on the design of academic qualifications,

which are likewise offered competitively. International students can bring high fees, making courses viable and discharging internal obligations to bring in funding. As with above, the degree market operates both as competition between universities on reputation, for the best talent overall, and between *courses* to offer something novel. The most able students bring prestige and hence higher fees, thus the university can in turn use their reputation to compete for a sufficient uptake of places.

“Some members of staff think that the primary determining factor for applicants to MSc courses – and even more so for undergraduate courses – is the entry qualifications that they need to get in and the perceived ranking of the university in pecking orders, and that students will go as high up the ranking table as they can according to the qualifications they've got.”

[EDU66E-CL71]

As seen above, a cynic might look at the attempts to present the subject matter of a course as being more aligned with current fashion than is necessarily true, to improve *interesement*. More charitably, one might look more towards the instinct of one contributor to look to find a unique selling point in order to stand out in a crowded market place. Whilst universities might *en bloc* be the OPP to “security graduate” status, individually this is not the case, thus a more esoteric course gives the opportunity to become OPP to that unique set of skills (albeit at a cost of potentially alienating the generalist, unless a more standard course is offered alongside).

Unlike professional certifications, degrees make a claim to *deep, conceptual learning* which in turn justifies them being vocational and obligatory to practise, as they represent the fundamental truths of the trade. Too much attention to changeable laws renders them more comparable to training certificates than a timeless degree, and thus their position in the network can be destabilised by the more respected professional qualifications. The guardians of these courses will then be caught between wishing to ensure their students have sufficient knowledge to enter the workplace and not losing the mystique of academic rigour.

In addition, in a network where the academic is expected by their management to act as a pure seeker of lucre, they may pay lip service internally to their obligations but without ideological commitment. Academics will not all be natural salespeople.

“I think this is across the globe, I've seen gradually in the UK an attempt to commercialise education, and as an academic I don't particularly agree with this approach. I can't see students as consumers of education, I can see students as students.”

[EDU54E-CL11]

Like Callon's (1986) scallops, they may then tend to betray the university financiers, who may believe that course designers are reliably concerned with student intake numbers and

employability statistics, whereas some (as above) may look more to the reputation of their department and the purity of the academic content. Similar pressures are seen by those who wish to achieve external validation with a non-commercial rate of return. Those looking to put pressure onto the academic system may have to cope with both sets of alignments that were visible from this data.

5.4.4 Role

In the previous section, the concern of some of the practitioners that their qualification should be recognised internationally was noted. Who, then, is performing this recognition? What fundamentally is a qualification *for*?

This cannot have a uniform answer. As was observed above, the careers of the practitioners generally pre-dated specialist academic qualifications in security and in many cases even mid-career qualifications. Some also pre-dated what they felt to be security being treated seriously as a topic.

“Security was, in the 70s, really nothing more than cryptography.”

[PRO62E-PO74]

Surely therefore there will be a difference between how a qualification is perceived by a new entrant, where a vocational degree is available, and by those who have changed career but without any early opportunity to establish competence.

Information Security expansion according to this sample occurred gradually from around the 1970s onwards, as computing also expanded. This expansion is reviewed later, but most relevant here is the description given of security hiring practices prior to certification. The description is of security as a small and not necessarily outward-looking community whose members were known personally to each other. Recommendations could therefore be made on the basis of peer appraisal and informal assessment. As the community grew, this became unsustainable and thus this community sought a way to test competence.

“We founded it to answer the question, ‘How do you recognise a good Information Security professional?’ Precisely that question.”

[PRO62E-PO74]

Does this indicate a change to the “group” way of thinking? This question is in some ways valid but not especially compatible with the ontological approach; ANT discourages talk of homogenous and predictable group behaviour, however the analysis must consider the contents of the network to view its irreversibility. Strong networks continually reinforce themselves,

however any network which contains “hiring manager”, “certification” or similar must be vulnerable to change if those entities are subject to change. There is already a minority visible who are particularly open to using certification as a criterion. One finance-based contributor noted that he would expect a candidate for senior office to be certified and “would be very interested to find out why they haven't done it” [FIN99E-SM92]. This was an interesting position, given that many others felt such schemes were more useful for early-career practitioners who could not trade on their experience and career accomplishments and thus required some proof of credibility and competence.

Precisely what *level* of competence is attested to is difficult to assess. Unlike a qualification such as the Cisco CCIE, or perhaps the Royal College fellowships for medicine, there was no apparent comparable qualification which established advanced competence. Language such as *baseline* and *benchmark* predominated. The role of certifications therefore should be seen as evidence of having reached some minimum, basic standard of ability. It is presented as proof of a claim of skill and knowledge as verified by an independent body of knowledgeable peers. This immediately draws the question of why then it should not be mandatory, since a genuine test of competence by definition is achievable by a competent person.

To establish *why* a test of competence has a market, requires examination of the job roles available in security. Generally as seen above it is the role of security to police internal processes; to audit, to correct and to permit or deny. Mostly if security has won these powers it is because they have persuaded their senior management that they must “procure” security in some way, and that the OPP for this is their specialist team. As we will see later, however, this is a fragile network. Security’s strength tends to be transitory after the latest major incident (supported both by this study’s data and the literature review), with efficiency and profitable processes rapidly re-ascending the priority list afterwards. Management will tolerate a degree of interference from its security and audit function where it has no other choice, however at a local level the practitioners report resistance.

In ANT terms, this can be seen as a settled network with a firm interlocked array of components which have an interest in remaining in their current arrangement. An auditor attempting to change such an established network is competing with one of the established links and attempting to break into it. As the auditor probably has few assets in the existing network, unless they can insert themselves without affecting the main relationships and the insertion lessens some other threat, such as that of highly disruptive external management disciplinary action, the auditor has little to offer. Ultimately what the internal human actors need to achieve is continuation of employment and lack of management sanction. A security function which can

compel the network's own hierarchical setup might therefore have a coercive power, and this indeed may be necessary.

But to use such a lever implies that the auditor or security analyst is absolutely sure of their ground, requiring confidence. In some scenarios where outcomes are binary and the auditor's decision is unlikely to be challengeable this has little controversy. Security however, as was established in the literature review, is very strongly related to risk management, balancing cost of action against penalties. These cost decisions are those of a generalist auditor and questioned by operations specialists who bear those costs; that decision is therefore legitimately arguable. The audit-trained practitioners stated that they derived considerable confidence and authority from their certification, which transformed their *opinion* into *professional judgement*.

It is possible therefore that although the certification acts on the network, it does not interact *directly* with the internal peer or client, unlike scenarios such as medicine where that certification plays a *major* role in convincing the client of the expertise of the professional. Why? Many practitioners spoke of the certification proving competence and establishing standing in front of internal clients. This was indeed the major theme after the role in securing eligibility for employment, but did not advance a mechanism of action. On the face of it, a black box might be imagined: certification as a reference to "Professional Status" or some analogue of it; an unarguable touchstone which anchors the otherwise subjective position of the individual, by inheriting the gravitas and technical infallibility of the apparatus of professionalism. And indeed there was some evidence of this.

"That's a key thing for me, it's partly to put on your business card and on emails and things like that, it makes you look more professional, whatever that may mean, but it does imply that you do know the subject; you understand."

[MAN61E-SM05]

This would produce a network as shown in Fig. 14.

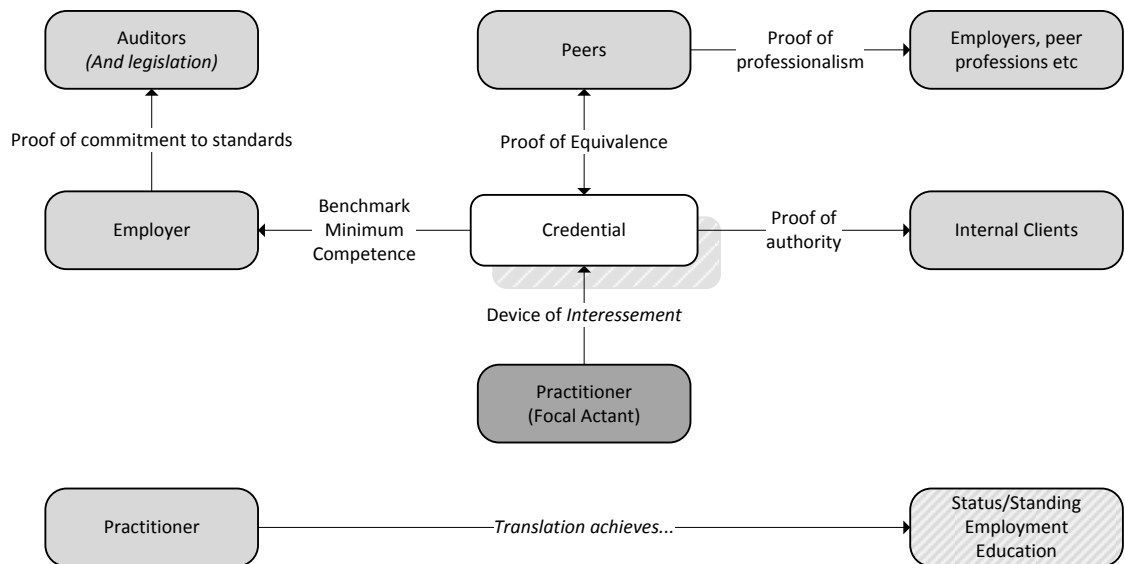


Fig. 14: Network as inferred from the perspective of the practitioner.

This must be challenged, however. In not all cases will someone's qualifications be visibly displayed. Immediate peers *may* be aware of the certification, however it is unlikely that others in the organisation, particularly during an audit or similar situation, would be presented with evidence of a qualification as part of their introduction. It was also apparent from the interviews that most non-specialists were perceived to not particularly recognise the separate existence of Information Security and hence would have no frame of reference for assessing the skill even of a credentialed person, yet this was a continual theme.

“And also the recognition of your peers, to know that you do actually know what you're talking about, you do know what you're doing.”

[TEC11S-ID48]

Where certification appears to have its greatest effect then is in *confidence*, particularly notable when juxtaposed with the lack of formal training in the current set of practitioners, which would tend to undermine confidence when dealing with qualified internal expert clients. The certification also proves to employers that their employee is qualified and is the gateway to the staff profile required. The status and understanding of the occupation from the perspective of those trades closest to security is sufficient to allow the certification to directly carry weight. This is in some ways the aim of the certification.

“My aim is to get people who have [our certification] recognised and valued, because it's an indication of commitment, knowledge, expertise, skills and so on.”

[PRO29E-PO42]

Outside this immediate circle, it seems more likely from the data that the credential creates self-

confidence in the practitioner during the negotiation of any changes to the existing network which might be necessary. The linkages themselves however suggest that the practitioner has the extended authority of senior management, and thus an implied authority through the hierarchy. Since the other participants' own hierarchical superiors will have been a part of the original settled network, the practitioner is competing with the existing arrangements to become the OPP to a satisfied management structure, as shown in Fig. 15.

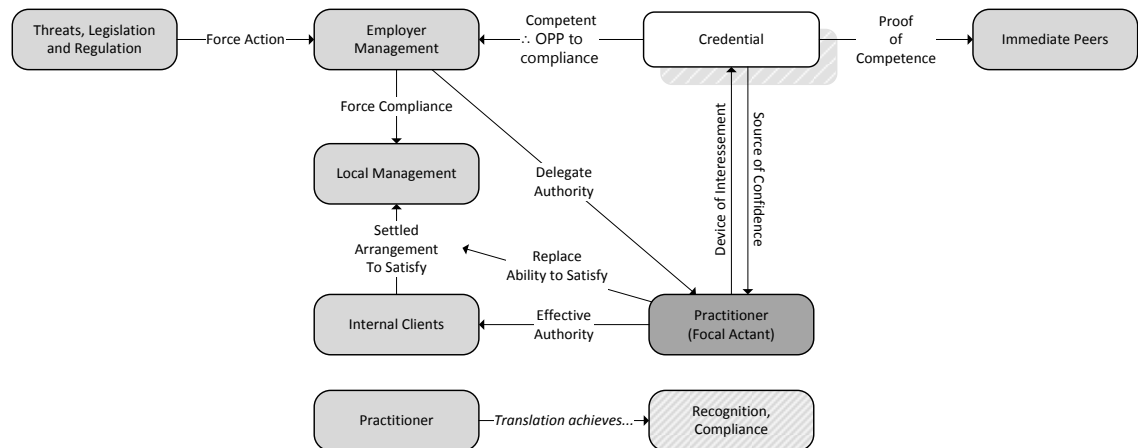


Fig. 15: Modified network seen from the perspective of the practitioner.

Certification was also seen to have positive effects on the perception of the occupation itself, whereby the actual physical presence of a credential implied the system of preparation and examination common to other professions whose authority could then be referenced as part of the presented claim. This is in some ways similar to the alleged action of scientists referencing previous papers as a form of *foundation-building* (see Latour, 1987).

“Certifications are important because from a professional point of view it puts across the right message that we're actually organised and we're structured. We have professional bodies that promote what we do, and actually measure what we do.”

[FIN91E-SM15]

Seen next to the quote from PRO29E-PO42 above, it is clear that the professional bodies and practitioners generally may well benefit from this increased perceived status, which will tend to add to the strength of the bond between the practitioners and the professional body. The more “professional status” is seen to be associated with certification, the clearer the role of the professional body becomes in the problematisation and the stronger the *interessement*. Interestingly, as in the previous section, having too many qualifications was seen to lower the perceived status of all, since a plethora of certificates weakened the claim of there existing a single state of being “qualified”.

Alongside competence, the aspects of *commitment* and *intent* were more prominent in the data than in the literature. Undertaking a certification is a demonstration to a potential employer that a person is serious in their career. In a world where security has not established itself fully as a completely separate profession which requires vocational training, this was seen to show that the job candidate had invested significant time in their own development.

“...to be able to demonstrate to potential employers that I had actually invested time and effort to attain a degree of proficiency.”

[CHA33M-SM54]

The undertaking of a certification process in order to learn new material rather than simply demonstrate mastery of it was also mentioned. Several late-career entrants noted a chance encounter with security but then voraciously reading into the subject during preparation for certification. Combined with the Continuing Professional Development aspects, this translated to potential for importing best practice into organisations. Association with best practice means that the *gravitas* of the profession can be drawn upon to compel a client to accept the judgement of the security manager.

Personal development then, rather than financial gain? One provider noted that people possessing their certification are on average more highly paid, however this wasn't mentioned by the practitioners to any noticeable degree as a motivation. One reported an increased salary as a pleasant *post hoc* benefit but was apparently not aware of this potential beforehand. There will be reticence towards admitting such a self-interested motivation, however this could have been done with reference to others or in some de-personalised way and this was also not seen. There were some general suggestions of being “good for one's career” or similar sentiment, however outright financial gain was not seen to be a particular benefit and this seems more likely to have been meant in terms of hierarchical promotion or quality of projects undertaken. This is not to suggest that the security community is a selfless collection of people working for the greater good; it is more likely that they simply do not equate certification to significantly higher salary. An exception was in the arena of contracting, where recruitment of a consultant was seen to be far more a question of obtaining a commodity and hence a benchmark was required to assure a minimum quality to the services being procured.

The employers in this network (either the interviewees' managers or their own role as senior staff) were looking to encourage certification. Although they could use certified staff to meet some internal or external customer demand, this seemed relatively minor compared to the desire of the security team to have employees with a formal development and education programme as part of normal personnel management.

“[We] are doing our CISM trainer in a few weeks; that's part of our commitment to the business to continue our professional development, but also the business has given it to us. They're investing in us from a career perspective.”

[MAN61E-SM05]

“Employer” as a concept requires some additional inspection. The practitioners in this study were mostly hiring managers and were able to describe some of that hiring process, particularly with regards to the balance of experience, qualification, social skills, technical prowess and so on being sought. Unpacking this, or rather de-coupling “employer” from one of the internal forces at work during recruitment, they were also able to suggest that prior to the hiring manager making a determination at interview, HR departments and recruiters were keen to find a way to sift applications quickly. Given that the hiring managers did not always support this where the claim of competence could be validly made in other ways, this breaks down any notion of “the employer” as a unit acting in a particular and unified manner. Similarly, it may be commercially expedient for an organisation to have “qualified” security staff in order to claim competently-managed security processes should their customers be felt to favour such things, even if the security manager would prefer not to put such an emphasis on qualifications.

“In the local government environment, those qualifications help to demonstrate to the various governance bodies we have to deal with that the council's taking security seriously, in that they're hiring qualified people to do the job.”

[GOV21E-DM38]

Such motivations of course do not represent a commitment to the substance of the qualification, only the badge, therefore this might not be coupled with board-level intent to genuinely secure the organisation's information or impart resources to the security function, merely to obtain a benefit through meeting some criteria. This particular network fragment would therefore be only superficially assembled, and would be vulnerable should the market conditions (or even one key contract) vary. In particular, conflict could even be seen if undertaking the certification brought in the *Iron Cage* effect (DiMaggio and Powell, 1983), with the professionals insisting on best practice from outside rather than acting purely as an employee (behaviour which was criticised by one of the contributors).

By breaking into “employer” further, evidence is provided for the credentials as due diligence mechanisms which was theorised as a network fragment above. There is an opportunity for other actors to affect the credential market for their own purposes, for example senior management.

“If someone employs a CISSP qualified or certified practitioner or whatever they can say ‘I did that, I've covered my back.’”

[MAN86E-DS66]

Similarly, an auditor who has to come to a determination of a security team’s effectiveness can appeal to a common agreement that there is a standard at play. For the professional bodies this gives another potential avenue to market; if they cannot convince the current practitioner set that qualification is vital, is it possible to convince the rest of the network to create a qualified-practitioner role which they are forced to fill?

“I saw a lot of contracts where it said ... ‘The Information Security Manager will hold [our credential] or equivalent’. So that was nice from [our] perspective. What that is, it’s a way of signalling to the supplier, ‘If you’re serious about this contract and security, you’re going to have people who have something I recognise’. Again, with contracts and procurement people they don’t care what security is, they don’t care what [our credential] is, they will go and check does it have this role – tick – does he have that qualification – tick.”

[PRO29E-PO42]

Examining and opening the “employer” entity gives a network expansion as shown in Fig. 16.

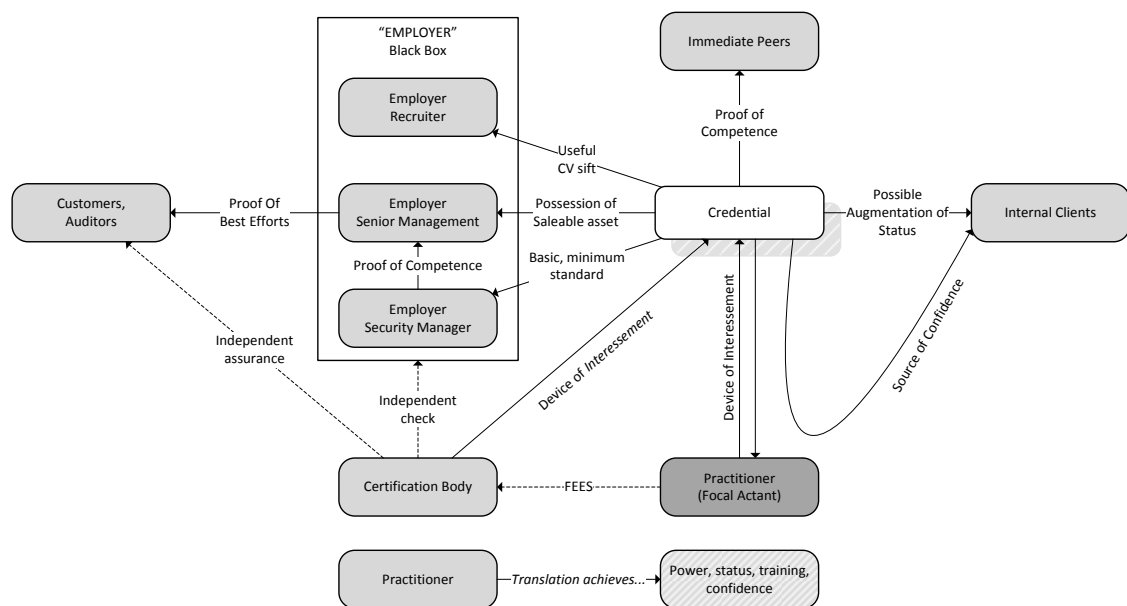


Fig. 16: Credential network from the perspective of the practitioner.

5.5 Professionalism

5.5.1 Overview

As was seen from the discussion of certification, the various actants have not completed the professionalisation project which can be predicted from theory as shown in Fig. 17.

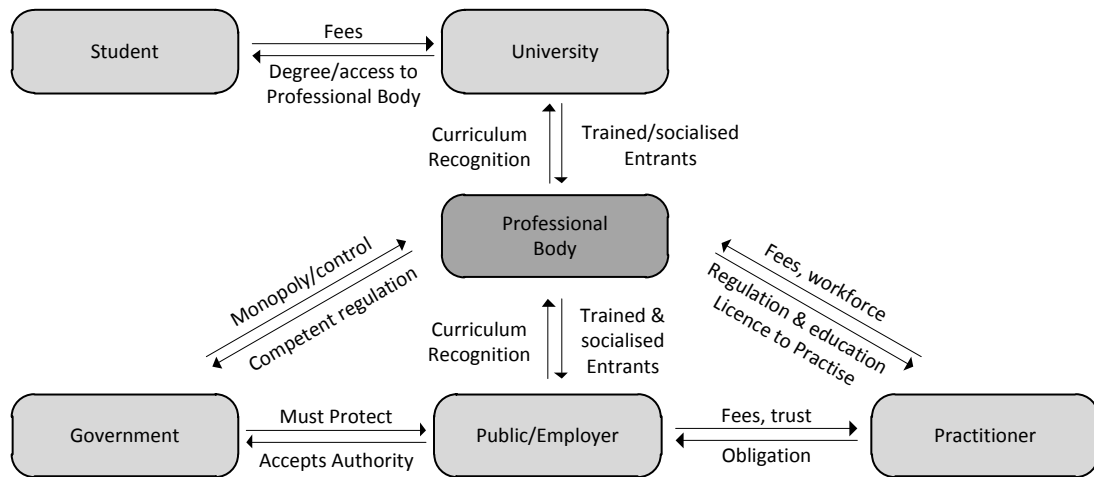


Fig. 17: Representation of a partial traditional professional status network (unified body).

In order to investigate further where the failure mode exists in this network formation, this section aims to examine these concepts of *professionalism* in the data. As no clear definition of professional status exists, to describe the progress of any campaign requires an understanding of what would actually represent success. It must be established whether:

- the practitioners who would need to be represented,
- the actors attempting to represent and ultimately enrol the professionals, and
- those who might regulate that process

all share a *common understanding* of the concepts, and whether professionalisation is desirable.

Four categories emerged during the analysis: what actually *is* a professional and how do they behave, the desirability of licensing, the role of government and the current professional status of Information Security.

5.5.2 Definition and Characteristics

There was little controversy over what constitutes a professional in the traditional sense, the group reciting the orthodox model when asked to define the term. It was seen positively overall and a status to be *in general* respected and sought, although not necessarily something with which this group particularly identified nor aspired to themselves. It was associated with seniority, at times both over subordinate trades of lower skill, and within the hierarchy of the profession. A rather egalitarian theme was expressed, particularly in the educators and practitioners, whereby models of profession which maintained a difference between profession and trade were rejected.

The most common traits mentioned were: adherence to ethical principles, advanced and specialist knowledge, competence (ideally qualified, although this was less prominent), and experience. The existence of a body of knowledge, a governing body, graduate training and application of abstract knowledge to a client's concerns were minor additional themes. The concept of professional purely as someone paid to do any activity was surprisingly minor.

No striking difference was observed between practitioners, educators and governance bodies, however significantly the government response was unusual:

“...a body of knowledge, it's got some sort of ethics, it's got development pathways, it's got a community, it's got a clear set of skills that are needed.”

[GOV01E-GV01]

That interviewee went on to draw very heavily on comparisons with medicine – the epitome of regulated and qualified practice – for his concepts of profession. As will be seen later, most practitioners distanced themselves from claiming anything like equal status to medicine.

Competence was a far higher theme than outright qualification (implying that competence could exist aside from a formal examination) and the question of *status* itself was not particularly pressing. For practitioners in particular, experience and competence were linked rather than qualification and competence. As was noted above, many such qualifications were created after their entry to the profession. The traditional professional network model as shown in Fig. 17 is attacked at this point. The black box of “professional status” as being a highly desirable and objectively attested state of competence (Fig. 18) is much less powerful in this arrangement.

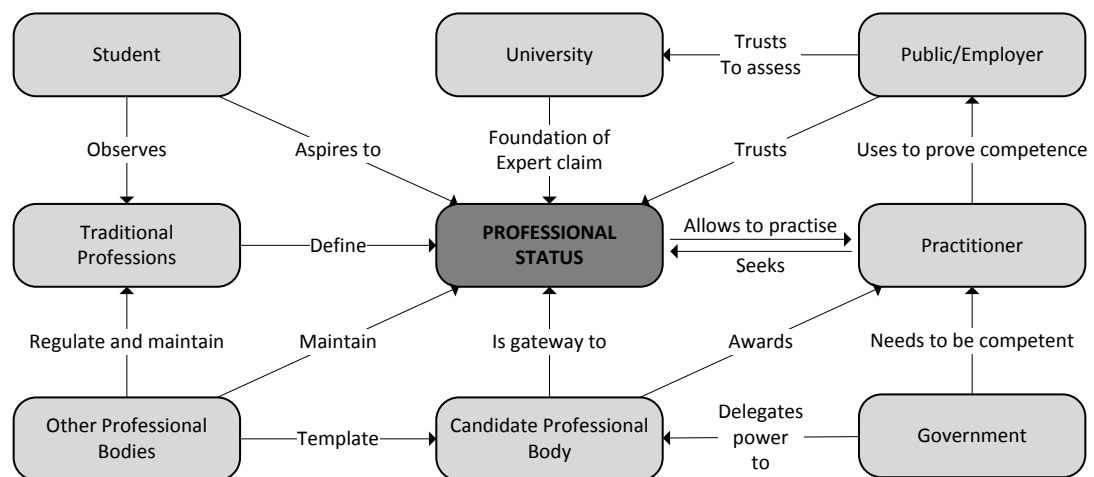


Fig. 18: Representation of professional status as the nexus of a partial network.

The traditional model implies that such status is reasonably solid, although notable for many of

the respondents here was a hesitancy in answering questions about the definition of professional within Information Security. Indeed, the discussion was a source of much of the material coded under the housekeeping code “My thoughts on this subject are not fully formed”. As will be seen later, whilst some of the deliberation was due to the subject being novel, there was also uncertainty when defining what they believed was generally seen as “a professional” alongside their own *lived* definition which varied from it. This confusion was particularly evident when the participants were asked if *they* were professionals; some claimed to be professional but not in the strict orthodox sense which they had just described.

Ongoing professional development was seen by many as important, rooted in the scale and pace of change in the industry and industrial context rather than mimetic pressure from the standard professional model and practice; there was little mention of the “appearance of professional status”. There was some cynicism towards the question of enforcing this for those with qualifications however this was not especially prominent and most answers were positive in tone.

Very few people identified with a strict separation of *professions* and *trades*. A typical response, allied to Ritzer (1973), was:

“Listen, you can be the guy who empties the ashtrays, you can do that professionally or unprofessionally, that's up to you.”

[EDU79E-ID24]

This understanding of professional status weakens many of the links in Fig. 18; if degrees, certification, licensing and tacit government approval are *not* required and merely simple employment, best practice and apparent competence in a field are the criteria, then the network is ripe for attack. Similarly, if status is not a driver then the practitioner is not so easily driven by the professional body, which must then persuade rather than command. In one case a contributor even sounded apologetic for suggesting that call centre agents might not be seen as professional and was at pains to note the potential for sounding elitist. It appears that overtly *referring* to social employment strata is now countercultural.

Due to this failure of the “professional status” black box to represent the interests of the practitioners, the traditional model cannot easily succeed here. It must therefore be established whether changes in the network can and will be forcibly re-established by the only actant with the power to actually *compel* other actants: government.

5.5.3 Government

This section describes the role of government in the regulation of security, distinct from the benefits and challenges of licensing itself (covered below). Much of this was contributed by the government interviewee due to directed questioning informed by earlier interviews, however one strand stood out generally, viz. reluctance for the government to directly regulate Information Security.

Contrasting motives for this were seen; the most striking being scrupulous fairness from the government itself, who felt it should not prefer one body over another because it had no business doing so, provided the market was consistent. It is therefore clearly not currently convinced that the impact of incompetent practice exceeds the cost of monopoly. This is hugely important given the power of this actor and the importance of state sanction for professional bodies. One professional body felt that government intervention would stifle change, setting the *status quo* in stone. Another felt that governments were not trusted by the profession to administer regulation competently, even suggesting that government backing would be unwelcome if they were seen to be the government's proxy. According to that thesis, if a body could not command respect on its own merits, it ought not to have it. In terms of the traditional professional network, this is also highly significant. Whereas in other professions government action is seen as recognising the pre-eminence of the body which represents the voice of the profession, in this case no such group representation has been fully established and thus state recognition of it would be precipitate.

The government's position suggests the lack of an obvious nucleus to which delegation could occur. Since policy is mainly driven at the political level, if change is not strongly desired from within it would need to be imposed by ministers. The topic was clearly not on the agenda internally, as many answers indicated directly or indirectly that this was not a topic which had been discussed extensively. Where the position was clear, it was that security was not necessarily a discipline itself requiring its own professional body, rather that it should be included as part of the regulation of the relevant industry. The likes of Ofgem in the network directly acting to control a profession would not have been predicted by the literature and were not mentioned by the practitioners, thus again this is a striking finding.

Government however has been far from idle, its actions being driven by a need to increase the supply of competent security staff. It will therefore tend pragmatically to pull *any* convenient lever, rather than its actions arising from a campaign driven ideologically according to some fixed goal. There was a clear sense that a test of skills should be available, however this was apparently driven in response to external requests for the government to define such a test,

which was delegated to the market, as the government had no mechanism to build and administer such a test itself. Additionally this was felt to be useful in raising competence levels generally.

“[If ministers never introduce regulation] then that's not the end of the world because you're encouraging people to use people with the right skills and the right competence”
[GOV01E-GV01]

The role of the government's professionalisation group was seen as ensuring its own protection through standards within government, and in the national infrastructure for which it was vicariously liable; as part of the civil service it has limited ability to impose its wishes on others without political instruction. The black box of “government” from the professionalism texts opens on inspection to reveal that it does not function as an integrated unit which “has power”.

This section of the network appears only to be in the stage of *problematism*. The actants are declaring their ground and establishing causes between each other with various aims and devices of *interessment*, however at the moment the government has not been successfully enrolled (lobbied to introduce licensing) and hence the key aspect of the translation is missing. In the following section that key as-yet failed translation is examined: power delegated from government to a “spokesman” professional body in order to regulate the profession.

5.5.4 Licensing

It might be inferred from coding values for this section (see Appendix 2) that licensing the profession was well-supported, however the reality is more balanced.

The educators were unanimously in favour, some strongly.

“I would see that as very positive. I would see that as very positive. Some kind of chartered status I think would be very useful.”
[EDU27E-CL05]

Similarly two of the three professional bodies were in favour, although not with the enthusiasm which might be predicted from theory; these were no passionate agitators to “exclude the quacks”. The third emphasised the need for a reliable badge but was not convinced it should be *imposed* universally. For the traditional professional network in Fig. 17, this represents far less support for actively promoting and advancing their power than might be assumed.

Contrary to the inherently monopolistic assertion of theory, when asked whether there were incompetent people in the field, some interviewees accepted that there presumably were, however the predicted rhetoric of *exclusion* was not observed; few considered incompetence to

be a pressing problem. If this is a general view and shared by those in government, this strongly attacks the orthodox network model, since it undermines a professional association being the gateway to a competent profession. One professional association noted that identifying the competent was a theme in the development of their own foundation, however this was during a discussion of the very beginning of the practice. Moreover, *not* excluding current practitioners was a *condition* for supporting licensing for many. The respect gained from professional status was not seen as a primary motivating factor for entry; relatively well-rewarded, stable and interesting work were seen as more relevant factors by the educators with regards to student entrants. The government interviewee was personally in favour of some form of licensing, however felt this was not imminent given that role definitions are still insufficiently defined. Along with several practitioners, there was also concern for the financial and administrative overhead which might be generated by such a move.

Practitioners were more balanced. Several were somewhat positive towards the concept but few unequivocally so and others were implacably opposed. A professional body would need to persuade more of the occupation than at present, otherwise it could present itself as a spokesman for a profession which in fact it did not reliably represent. Much seems to depend on the detail; a code capturing, effectively, *conditions for accepting licensing* proved fruitful. Concerns centred around the practicality of introducing such a scheme. What knowledge was to be mandatory? At what level? Who would administer it? How would one amass experience if it were necessary to have an experience-based qualification to enter? These obstacles were not insurmountable; if a scheme were to be introduced which the practitioners felt reflected the correct mix of skills and areas of knowledge then the uncertainty around what was proposed would likely decrease.

5.5.5 Status and Direction

Professional status is a curious phenomenon which must be examined more closely.

There is today widespread use of “professional” and “pro” not only as making a living from a trade – particularly one of the vocational graduate trades – but also as a marketing device. Items such as shampoo sold as “professional” but clearly for domestic use suggest suitability for the advanced user aiming for the higher *quality* which professionals produce. One might consider the term “professional” to be an inscription, in that it has a common but nebulous definition written into the network by repetition, which needs only to be referenced to allude to high levels of skill, judgement and reliably high quality of output, without detailed examination of the exact claim.

It is however *both simultaneously and conversely* used by some as a more formal term for those trades for which qualification is by graduate study and subsequent postgraduate industry qualification; this sense is still *very much alive* for some. Its *exact* definition for this sense is dependent on current perceptions of the term, but distorted by the gravitas of the prototypes in the field, thus the perceptions of professionalism and what it means to be *a* professional (as represented in Fig. 19) are very much part of the network rather than mere intermediaries.

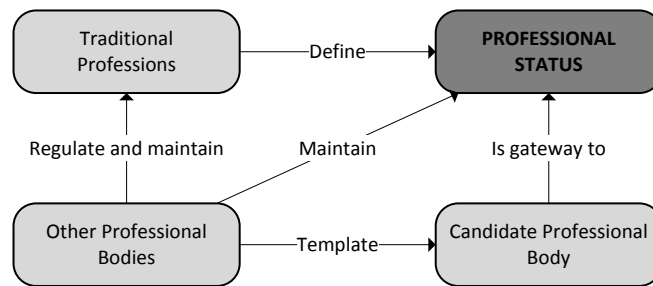


Fig. 19: Partial view of an orthodox model of professional status.

If “professional” can be simply mentioned to denote a tool brand’s halo model, promise high-quality electrical installation or attest to post-graduate practice-based qualification, it has become a black box: punctualised and used without explanation or examination. But translation here is incomplete; no professional body has control, which demands that the *unpacking of* that box to explain the network weakness. Which style of profession is referenced by professional certifications in Information Security? To be enrolled by a professional body practitioners must themselves want to obtain that professional status, but what elements *for them* comprise that status? What are the demands which a professional body must answer to avoid network weakness and thus fail to achieve translation? Since other professions’ identities shape those impressions, they too are at large in the network.

The prevailing impression was that Information Security is too specialist and emerged too recently to be accepted as a profession in the *traditional* sense. To the layperson, the practitioner’s services are unclear, forming part of IT or the corporate police force. Lack of status to the layman is significant; to this group, contact with the public means exposure and thus an identity in the public mind, and consequently status. This would suggest that the public perception of professionalism is another entity affecting the network, which again is affected by perceptions of the other traditional professions.

This makes for an interesting aside for the theorist; Freidson (1970, pp.21–22), for example, makes a distinction between consulting and technology professions. Whereas medics are required to have status in the eyes of the laity, technical specialists need only be respected by

peers. To Abbot (1988, p.118), working with the public directly is distasteful; senior professionals delegate this to juniors, or entire junior professions (barristers to solicitors and doctors to nurses, for example). Professional status for these people was associated with a high impact of incompetence, particularly as support for the paramount position of medicine.

“I think the stakes are much higher for a doctor. No marketing professional’s going to kill a load of people if they get it wrong.”

[CHA33M-SM54]

Potentially, this limits the ambition of practitioners seeking that status. Two people however, a professional body and the government interviewee, noted that security *was* moving towards protecting personally significant interests and safety, as more systems were entrusted to electronic operation, thus this may support future changes.

“Safety is now reliant so much on security, safety for many many years has looked at as component failure and hazards like weather and all that kind of stuff, but it doesn't include malicious action. And we're seeing more and more malicious action which will now affect safety.”

[GOV01E-GV01]

Public perception of absolute status was not the most notable issue. Rather it was the distinction itself – the crystallisation of discrete roles and identities within professions and the hierarchy between the professions themselves – which was seen as crucial. Whilst these professions are seen to have well-established roles with formal paths to qualification, the career path and “rank structure” of Information Security is not seen to be present, for good or bad.

“Again, I go back to medicine; there's lots of specialisms in medicine that have developed over many years but everybody agrees that a neurologist does things with the brain and not with the kidney. I don't think we're in that position.”

[GOV01E-GOV]

This lack of clear terminology creates a difficulty in making comparisons between employment roles, which in turn complicates the process of qualification and makes the claim of representing a discrete and identifiable profession difficult. One of the principal challenges to regulation and greater organisation was thus held to be drawing the boundary around the profession, something which Abbot (1988) suggests is a dynamic process over time as adjacent professions jostle for control. Without that boundary it is difficult to select and enrol a discrete set of actors.

The question of coherence was seeded from the literature, given the efforts to codify roles. One line of questioning was the broadness of the different skill sets; whether for example a forensic analyst or firewall engineer was part of the same profession as someone who creates policy or educates an end-user. As seen earlier, the literature strongly suggests this to be the case. Two

educationalists saw technical and policy aspects as separate professions, however generally this sample simply noted the complexity of the current status without advancing any potential ideological boundaries.

“So while everyone can have quite distinct roles, you actually need all of them to make it work. ... [Y]our elliptical curve cryptography person knows everything about how to encrypt something and decrypt it but doesn't necessarily understand the wider context of why you might need to do it.”

[TEC72E-AN91]

It is noteworthy that several people mentioned the IISP Skills Framework as a factor for change, either usefully to define the roles and hence education paths for those roles, or less usefully as a constricting force which does not reflect the less predictable course of a typical business career. Either way this typography of roles is generating comment in the industry, potentially representing an inscription in the network, accepted without further discussion as a role reified: a physical symbol for its contents. Such entities are useful for creating stable networks, since a network whose base elements are constantly having to re-assert themselves against challenge will be weak.

Overwhelmingly the perception was that whilst not yet complete, Information Security had the potential to become (or even *should be*) recognised as a profession; it was felt to have sufficient intellectual depth, but had not yet achieved matching gravitas and status of more structured examples. It was almost unanimous that a CISO would not enjoy equal status to a company lawyer; government noted that it sought actively to improve this status, not being particularly high, otherwise there was no clear difference on this point between the source types.

The above does not imply zero status for all practitioners; status is simply won by the individual, assisted by job title, hierarchical seniority and perceived personal competence. By contrast it was felt that “recognised” professionals command *automatic* respect; their claims are accepted in the network by reference to the status of their profession alone. ANT here shows the power of non-human actants; whatever the motivation of physicians to advance their *own* status, without any likely intentionality on the part of the human doctor the status of their profession has effect in a distant, almost unrelated network.

“Medicine's another great example. Doctors, medical students spend two years basically in a classroom where they learn how the human body works. ... They start off with a broad knowledge, and they narrow down, because the principles work no matter where you are.”

[PRO29E-PO42]

Exceeding even obscurity and the lack of structured roles and qualification was a perceived lack

of maturity and history, charmingly expressed as “It's not old enough. Doesn't even have a nice building in London” [GOV01E-GV01]. The “heritage” of other professions *qua* profession was arguably over-estimated; interviewees spoke of medicine as having “hundreds of years” or “millenia” of history, whereas Freidson (1970, pp.5–21) places a recognisable medical profession no earlier than the end of the nineteenth century. The black-boxed status invokes a sense of ancient foundation which would not withstand unpacking.

“Security *is where medicine was many hundreds of years ago*, in that we apply treatments that sometimes work and sometimes don't, and we don't always know why.”
[GOV01E-GV01, emphasis added]

Security was seen to be less mature and of a lower status even than the more modern examples mentioned in the interview protocol (pharmacy, nursing and engineering). Two perceptive voices challenged the question, denying the implied recent emergence of engineering. One noted that civil engineering prior to its professionalisation dated back to Roman times and another noted that engineers were socially prominent in the Victorian era but did not protect their status (notably similar to Larson's (1977, pp.25–31) treatment of engineering). It is apparently *perception* of maturity which influenced the sample and thus against which offers of representation by a professional body will be judged, both by practitioners and government, made more difficult by the short history of information processing.

“The technology we work on has only really been around since 1945. It's transforming itself every two or three years, so we are playing catch-up in a way that other professions never had to.”
[PRO29E-PO42]

One professional body noted that they had an aim to be more comparable to other professions, however another aimed not to be of equal status so much as being equally well-organised and ethically practised. Again, the perception of the other professions clearly has a strong bearing on what would be required in a regulated network. These comparisons hinted for example at the direction the speaker saw for the occupation.

“Security ... is still seen as something you can spend three years doing as part of your overall career. Of course yes in three years you might become a bottom-end GP in medical terms if you're lucky but the reality is it'll take you many years to become a specialist.”
[GOV01E-GOV]

As an aside, it is most interesting that the government interviewee should criticise this sense of not requiring specialised knowledge but strongly resist the profession being licensed as discussed in other sections.

In terms of structure, the practitioners in the main felt that whilst an earlier IT career provides

important technical grounding for key areas of policy enforcement, career background should not necessarily determine potential. Earlier sections showed that the practitioners similarly refuse to insist on graduate education, something which the educators naturally consider to be a natural foundation for a career. One person noted that the general increase in popularity of university education may (once more) require a person to be a graduate in order to be considered a professional in future. The sense here was that this stemmed from the statistics of modern practice and custom rather than a phenomenological analysis of the essence of profession.

Looking to the future, it was felt that the role itself will change. One practitioner predicted that recruitment will be from a much wider variety of skill types; this made an interesting contrast to the government (DBIS, 2014a) view that more entrants with STEM subjects are needed, suggesting a continuing technical bias. All parties agreed on the lack of competent staff in the market and the importance of increasing the supply to the industry of trained staff.

“We're [producing graduates at] way below the amount of people required to cover this kind of role.”

[EDU54-CL11]

As the government has recognised this, in theory this creates the conditions where it may wish to delegate the task of regulation.

5.6 Work Context

5.6.1 Overview

This final section places the candidate profession into its work context in order to extend the partial network observed above. The causes of the change around the topic of security are noted to determine which are the genuine actants exerting influence in the field. From this can be seen why security now occupies its current position and what might cause this to change. This is fundamental to an ANT study because it attempts to enumerate and describe the actors at work in creating the role, of whatever type. The security specialist exists in an employing organisation, thus the network of interest is that which gave birth to the object of study.

The question of security's place in the organisation is also examined to note the degree to which it has established itself into the hierarchy and how effectively it has distanced itself from its IT-dominated history. In particular, it is necessary to establish whether the practitioners respectively of policy creation and policy enforcement represent strata, kin or discrete atomic trades. Next how the profession is perceived internally is seen, particularly with regards to its

management, who represent in a bureaucracy the profession's clients as traditionally described. Finally the relationship between policy creators and those affected by it is discussed, to see how these people feed back into the policy process and hence fill out the remaining parts of the network.

5.6.2 Change Actors

Whilst it is convenient to refer to "legislation and regulation", this varies both in scope and context, thus these must be placed into the network with care. These are casually referenced as major sources of change, suggesting this concept has become a weak black box. Weak, because invoking it lazily by a practitioner (for example to gain funding) would withstand little scrutiny by a determined counter-force in the organisation.

"In retail it evolved as the time went by and regulatory requirements were one of the drivers for that. Here that's not so much the case; there are no such regulatory requirements that compel us to comply with anything on the security front, really."

[MAN61E-SM05]

This statement makes the assertion by government that security should be regulated not as a whole but by sector very interesting, since it is clear that this would then vary enormously between industries. There are numerous regulatory pressures which were noted by the interviewees. PCI-DSS was seen to have almost statutory effect in merchants; interestingly a charity pointed out that they were equally bound by such concerns, but battled an internal assumption that charitable status somehow reduced them. Finance mentioned enforceable regulatory action as a key source of concern, whereas a Health Service interviewee noted the balance of data protection against critically high availability requirements for authorised use in the subject's vital interests.

"I think that depends on industry. In retail I think they just pay lip service [whereas] in the gambling company a lot of resource, a lot of money. Pretty much got what I wanted."

[FIN22E-AN43]

Whilst security must reflect the actual threat to the client, thus some variation is natural, there could surely be no homogenous profession with such a wide difference in approach and internal priority, if regulated according to industry type. Such differences create tension between the profession-aligned practitioner and the employer, leading to conflict in the professional concerning priorities and best practice (DiMaggio and Powell, 1983).

"The emphasis is on the information governance, it's about patient personal identifiable information. The rest of Information Security is definitely secondary. *And I find that difficult.*"

The single contributor from a small organisation felt that enterprise size was a significant factor in behaviour. Here the importance of agility and flexibility was paramount, with security measures facing stringent assessment to ensure no impact to profitability. Resistance to security restrictions from senior management is likely to be particularly acute and the security officer (possibly a hybrid IT position) would therefore require more support from external sources. Another participant suggested that those aiming to avoid security constraints might avoid hiring security officers known to favour operational intervention.

“Actually it depends on the sector. I mean, lots of small businesses just generally don't care, as long as they can get on with the job they don't care.”

[TEC11S-ID48]

Parallels between security practice and Health and Safety were noted, the latter probably most closely associated for UK workers with the Health and Safety at Work etc. Act (1974). Through such acts society embeds into law that neither public nor private enterprise may, in the pursuit of its work, gamble unnecessarily with the wellbeing of staff, something which is now well-accepted.

“If you look at anything in here, everything you'll see is Health and Safety and that's number one. Has been and probably always will be. And justifiably so as well”

[MIN48E-SM22]

This has not always been the case, with the maiming of early industrial workers by unsafe working practices sewn into national lore. If the motive is assumed to be profit (additional resources required for safe procedures and equipment conflicting with maximum production) then clear similarities to security in business emerge. Overheads of procedures such as separation of duties or whitelisting of applications, or costs of equipment such as firewalls, conflict with the priorities of operational managers.

In both cases an economic argument exists both pre- and post-legislation. Society has chosen to consider risks to the person as unacceptable and skews the risk for company officers in favour of proper practice by the use of fines and the threat of imprisonment. Similarly security-related legislation, such as the Data Protection Acts, re-balances the risk–reward spectrum for directors. Where profit may encourage avoiding reasonable measures for the protection of personal data, the threat of fines may change the financial outlook, with personal criminal sanctions affecting risk calculations for executives even further.

Without legislative backing, pressures such as market reputation and the loss of intellectual property are risk decisions which can be taken (informed or otherwise) by the senior

management, thus the security officer has no power to direct upwards within the organisation. They must convince management that they are an OPP for a state which they may only weakly wish to achieve; should their cost be unacceptable or should conditions change, the network will remove them in favour of another focal actor.

With specialist legislation, not only must the management comply with the Act but it will not be sufficiently expert to know how this is possible or how to execute it, requiring an advisor. This therefore firms both the desirability of the target state for which they are OPP, but crucially also cements the degree to which they are genuinely the only passageway to that target. Should the firm operate in multiple markets, the degree of expert knowledge to claim OPP status is apparently increased still further as the international variations in such issues were seen hugely to complicate compliance.

For smaller organisations, the combination of fines and a more active commissioner's office was seen as effective. In larger companies where the maximum fine would not be catastrophic, reputational damage was held to be the primary mover. In the former case an overly-officious security officer would be susceptible to contradiction by legal staff; in the second judgement would be more pragmatic, having regard for market impact.

Standards, by contrast, have a more nuanced method of action. In theory they are not mandatory (aside from quasi-regulatory examples such as PCI-DSS). Backhouse *et al.* (2006) interestingly consider the standard *as OPP*, being the gateway towards acceptance by a customer as a bidder for work. But this is to mis-ascribe the focus of the action. The standard, as they note, is an artefact from a process where actors wished to achieve some purpose. Whilst adoption of standards might be fully voluntary (as one practitioner noted for example, external standards avoid detailed debates over each provision of a proprietary policy), for these practitioners adoption was usually for some specific purpose. As Backhouse *et al.* noted, this may or may not align with the stated motivations of its creators; adoption may instead be due to market-based mimesis, or expectation and custom rather than some objective benefit.

“We were also working with the [government], the web front end for the [public sector] recruitment site, so we had strong development practices in the business and we were used to having audits, but more and more companies were saying ‘You don't have the badge’, so we got the 27001; they were happy.”

[UTL50E-SM62]

If its adoption is through reference rather than substance therefore it is more likely not an OPP but an inscription: an item in the network accepted but never examined. Did the purchasing teams of customers who required this standard even know what was written in it? Almost

certainly not. The standard is a device of *interesement* during the problematisation phase of some other interaction. The customer is a gateway to money, and the supplier a gateway to secure services. The standard itself, regardless of its genesis, is adopted under these particular circumstances for its effect and punctualised: reduced to a badge. It is certified compliance which gains movement in the market, which is the product of an auditor.

If the standard itself is considered to be an OPP rather than an artefact, then the translation it achieves is a poor one; practitioners report complying only with the sections they actually support and do not cause undue effort unless forced. It is not clear whether this is due to the security manager being themselves unconvinced or a failure to translate this into internal action; there was evidence for both.

If adoption is not market-based compliance but due to the standard as actor, its interaction is with the security manager as spokesman for their internal network policy. Successfully lobbying the security manager of the benefits of compliance in its own right may appear to deliver results; in reality, though, lack of compulsion causes the standard to be unpacked into constituent actions, each with financial and resource costs and benefits.

“The majority of it's good but there's a small percentage of stuff which given a choice we probably wouldn't do.”

[TRN74E-SM47]

However enrolled the security manager, this will not further translate into action without a reason to comply with the *entire* standard being apparent to the resource managers. The security officer may even resist the implementation, since they will actually have to introduce it and may have lower respect for it after unpacking.

“It's a bit like ISO9000 to me ..., you can have a repeatable process, it can be a crap process but as long as it's repeatable, job's a good'un. I suppose the other side from a cynical perspective is that mandation [sic] – what's the driver behind that? Is it a revenue generation thing or is it a genuine desire to wish to increase the professionalism or the quality of what's being done out there?”

[MAN61E-SM05]

So what is the focal actant here? Standards compliance brings with it the customer as candidate actant. But as noted above, does the customer genuinely wish to see those exact measures, or have they been successfully enrolled in some other actant's power play and are merely reacting predictably to events? The customer seeks security; the fact that ISO standards are not mandatory in most cases ensures that this action is not *required* of the customer. Some other event has convinced them that engaging a secure supplier is a desirable state.

From the data collected (strongly in line with the literature), this appears to have its roots in the change in exploitation of computer coding vulnerabilities from theoretical exercise to malicious action.

“Before if you look at hacking in the 70s and 80s, those people were there for the kicks ... It was more of an intellectual challenge. ... [N]ow you have people that actually get paid to do this, if they manage to get your credit card number and personal information at home and your IP address at home they get real dollars in their bank accounts so now the motivation's completely different.”

[FIN99E-SM92]

Between these two extremes – principled hacker who would avoid damaging the target system and modern financially-motivated organised crime – the spur for security was seen to be the computer virus.

“[Security] wasn't in the least bit important to them, right up until they got smacked over the head by this virus.”

[CHA33M-SM54]

Interestingly this quote could apply equally to the epiphany in the IT department as well as the “proto” security officer, since the rise in malicious intent demanded properly-secured computer systems. It might be no coincidence that the introduction of computer security programmes by a small number of specialists and its academic study were seen to be contemporaneous with the outbreak of viruses.

Whether the virus incidents themselves were the principal factor here or the *perception of risk* is an interesting point. Clearly in large organisations security breaches themselves were damaging, however they were also newsworthy and helped create in the minds of the observer the abstract and general sense of danger from poor security.

“There's a lot more exposure, but that's not necessarily backed up with understanding. People say, ‘Oh yes, Information Security, I'm really worried about that’ but if you ask them what it is they won't be able to tell you, all they know is the scary headlines in the media.”

[CHA33M-SM54]

Again, the choice of focal actant requires some observation. Where there is the perception of danger uncoupled from a detailed understanding of the exact nature of that risk, an opportunity is created for a security officer role to become the OPP to achieving safety.

“But the publicity that cyber-threats get in the press, the publicity of incidents that have happened make them think twice, especially if the Information Security professional in the organisation is able to make the links with the risks to that specific company.”

[COM73E-AN44]

Interestingly, not all the focus was purely technical. There was also evidence of the later von Solms (2000) waves, in that businesses became interested not simply in responding to the information systems attacks, but also in some cases in creating proper process and structure around the organisation of secure practice itself.

“It became recognised that there wasn't enough governance, not enough control, not enough oversight and not enough resources in place to actually deal with the risk and impact. That's when businesses started to realise and actually do something about it.”

[FIN91E-SM15]

The participants were apparently not suggesting that this position and the attendant focus on security were created for ideological reasons or to protect data as a means in itself, although one telling aside relating to “bitter experience” suggested that there was some internal feedback mechanism. It was seen that this became a true topic of interest when a lack of security cost businesses money.

“As soon as money is involved and there's a threat of money being stolen and there being economic damage of any kind, then it becomes of mass interest.”

[EDU27E-CL05]

Viruses are an example of what one participant termed “this week's buzzword”. Led from the literature, questioning discussed whether reports of security breaches were used as a lever within the organisation. This was to establish views on this topic in general and then more particularly to elucidate what the mechanism of action was (greater access to executive risk aversion through fear of the breach, easier business case based on financial impacts in a rational assessment, and so on). In most cases this was rejected and seen as rather cynical behaviour. More pragmatically, it was noted that the threat would have to appear very close to home and that it was possible to cry wolf.

“I think people have used it as a catalyst to get attention but I think you only get a few opportunities of doing that before people get weary of the story.”

[FIN31E-AN72]

This latter point is significant. Much was made in the literature of professionals having *power* over clients; for that era of sociology a profession required *credibility*. The professionals may have been theoretically bound to higher things than their clients' whims, but surely only where a gentleman's income allowed some independence and the regulation by peers provided some shelter; clients were still ultimately paying their salary. The power school claimed no direct element of *force* to the mechanisms at play, rather that by having such great influence born of expertise and the credible nature of their warnings of the dire consequences of non-compliance, they had a coercive platform, and by controlling knowledge they controlled clients' options.

As was noted in the literature review, professionals are distinguished by giving advice with great penalties for disobedience: failure to listen to the lawyer resulted in loss of liberty; the doctor, death. As even Freidson (1988) noted, this is not however direct power like the Leviathan state; consequences of not following advice have effect only if they are perceived to be both real and sufficient. Advice from a competent lawyer must be accepted to avoid the legal sanctions they warn of, but even this cannot compel action from their client in the real sense, since some people are simply obstinate or self-destructive; the client retains their right to make bad choices.

To achieve similar power therefore, the security professional must credibly produce advice with a high cost to non-acceptance, if they are to be the OPP to avoiding that cost. There is therefore a fascinating tension in the answers observed here. On one hand, well-publicised breaches are known to affect executives' thinking and have an effect on access to funding and control within organisations. On the other, the data suggests (in line with the literature) that only when such events are recently in the mind of the management would security have their full focus. In some cases such incidents even *created* the department. This has some resonance with ANT, which rejects solid social "forces" and requires these negotiated links to be continually renewed.

Deliberately using this to gain resources was seen in the main as ineffective, because it would not map to the exact risks of the company and thus seem irrelevant. Secondly, even though breaches might get management attention for security, to exploit this for resources was seen as unethical. One *ethical* use suggested was as material for cautionary tales for awareness training, to communicate the nature of the threat. Whilst therefore breaches might be seen as actants, it appears their action is to amplify the effect of the user of the malicious code, which may or may not be its creator. Malware thus becomes a device and the breach a conduit and amplifier of action.

That malware was seen as so significant by practitioners is instructive; the emergence of viruses created both the functional need and the commercial case for Anti-Virus software, arguably the real foundation for the security product industry. One practitioner saw this as causing the preoccupation with technical mitigations, linking Information Security to IT controls. This contrasts with another view that the industry has moved away from constant development of novel technical controls towards creating services and suites, but the "noise" around the practice of security has continued to increase. Aside from this "noise", the impact of the security industry seen in the data was surprisingly small. Alongside noting the useful source of advice, there was some cynicism towards the "security theatre" attitude of the industry and their tendency to oversell.

“The very top-level executive people tend to not have any depth of understanding about the scale and complexity of the Information Security challenge. Some of the fault of that has to lie with the security industry for touting themselves as, ‘We are the answer to all your problems; all you do is sign this contract and everything’s fine’ or ‘Buy this box’ or ‘Hire our consultant’ or whatever.”

[CHA33M-SM54]

There was little other spontaneous mention of what is now a substantial industry. A possible research strand could focus on how its workers fit into the profession’s role hierarchy. Just as medical research is not solely performed by physicians, developing the technical controls used by practitioners represents a different environment from that of their application.

Whilst the practice of Information Security management is not exclusively a technical one, the data here supports the common view that the occupation’s origin is linked to the development of electronic computer communications and mass computer internetworking. It was the development of these additional vectors to compromise and exfiltration which seems to have separated the protection of stored information from that of any other physical asset. It also changed both the skill set for the thief and the danger of their being captured. But this is clearly not the limit of the impact of technological change; prior to social media for example the concept of an online identity could not exist to be misused. Whilst therefore the emergence and popularisation of Internet access is clearly fundamental to that of Information Security, this is such a well-documented phenomenon that little is achieved by rehearsing it here beyond noting that the interviewees’ data supported it. Thus the ANT duty to hear all things in their own words has been completed.

Far more interesting is to note the significance for many of the *pace of change*. This scene has been set in quite stark terms; people who knew the weight of the words said that at the beginning of their career, *security did not exist*. This brings in itself some interesting observations from the group. Firstly it was felt that change was so profound, relentless and rapid that it almost precludes any one individual from truly becoming and remaining a genuine *expert*. As a statement this can be debated, however for these purposes it is most relevant because a topic which cannot adequately be understood by an individual is ripe for specialisation, which speaks to the topic of occupational coherence. Secondly, it produces an obligation to undergo *bona fide* continuous professional development. Thirdly, the public image of the subject has not yet had sufficient time to react; public and management understanding of security topics cannot hope to keep pace with the development of the threat landscape without interpretation, thus there is a more firmly established role for that interpreter.

A similar generational change has happened in the client community. The industry is running to keep pace with topics such as protecting against external threats, perhaps for this sample best

exemplified by “Bring Your Own Device”, which was regularly discussed in the security media during the interview period. When a generation which had become accustomed to universal and unfiltered internet browsing collided with the traditionally conservative and prescriptive security function, a clash of ideologies was played out in the world of security policies and corporate politics (see Leuprecht *et al.*, 2016). Where management understanding of the threat is in error (and quite possibly also understanding of the perceived benefit), they may choose to bend to the insistent calls for a more liberal computing environment due to a faulty understanding of the balance of risks.

In ANT terms, the security officer’s position of OPP has been challenged because if they are not able to support the demanded flexibility and openness, they cease to be an apparent passage point at all to the desired end-state of a secure *but flexible and functional* computing function, thus the alternative path via a less intrusive regime is taken (shown in Fig. 20). Clearly in many cases this is because the security officer has been outpaced by movements in the network caused by technology, but in others it is because choices have been made without sufficient understanding of the risk.

To this school, the responsibility of the security officer is to engage with what functionality is demanded by the business customer and to find a way to provide it securely, so that they actually *enable* the operations objectives of the enterprise to be achieved. In addition, by providing training to the user, understanding of their policy position could be increased (creating empathy and ideally buy-in), and the user able to better protect their home environment, thus shifting the general appetite for derestricted usage and improving the political position of the function.

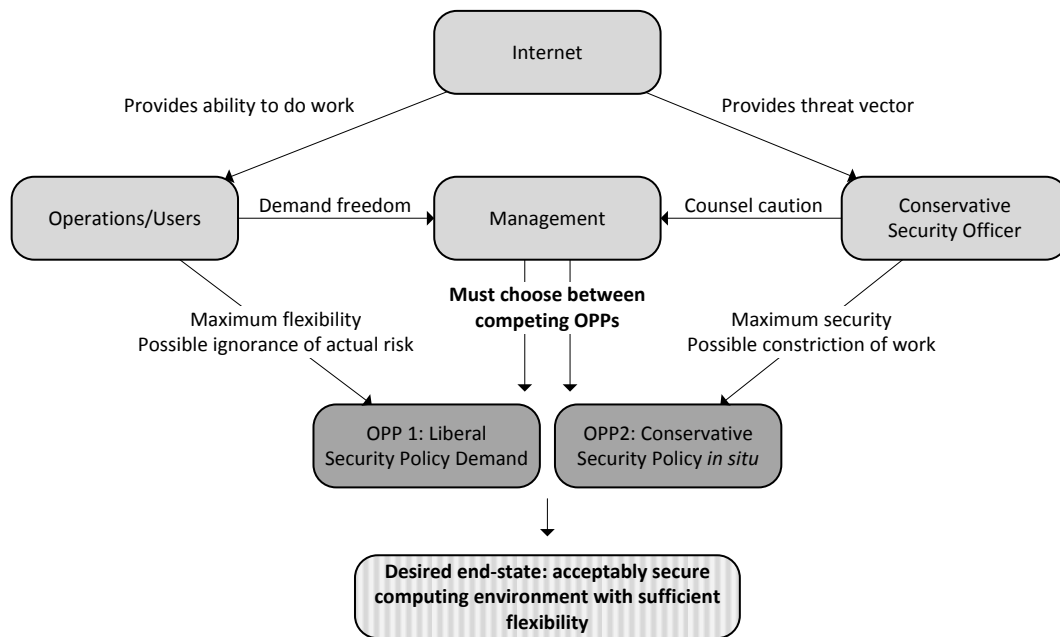


Fig. 20: Network instability caused by dissent to restrictions from security policy.

Obviously the most appropriate policy will depend strongly on the enterprise's sector and the nature of its operations (and hence threats). This data was therefore in accord with the literature in seeing sector-specific security contexts, but some interesting nuances were observed. It was mentioned that charities may see less ideological threat from anti-capitalism, however the organisation could still conflict strongly with dangerous external political actors. An environmental charity might be targeted after criticising an environmentally irresponsible state which had an offensive cyber capability, for example. As one interviewee noted, their regulatory environment (for example processing personal data and financial transactions) can be identical to commercial endeavours if the law does not distinguish, even though the internal funding available may be very different. Sector-specific principal threats also exist, for example health services mentioned the paramount importance of medical data confidentiality, particularly if exfiltration would result in costly legal action.

A further interesting suggestion was that some regulated sectors would be required and thus accustomed to employing *qualified* staff operationally (such as civil engineering) therefore internal staff would know and respect more the traditional professional model. In such organisations, a certified practitioner may be more easily accepted as a peer by internal clients through recognition of 'certification equalling competence'.

In summary, this section presents concepts relating to the creation and development of security practice as an enterprise role. From 1970s cryptography as the earliest observed action in the data, in less than fifty years there has arisen a discipline with vocational degrees and a

government campaign to recruit. Intrinsic to an ANT account however is the juxtaposition (network) of the actors described above. Latour (2005, pp.63–86) notes that neither hammer nor human of themselves place nails into walls; it is the interrelation of these objects for the moment of relation which produces the result. Similarly, the creators and creation of malware, the spread of the internet, the ubiquity of electronic communications and equipment, the publication of malware attack by the media, the vulnerabilities of popular software, the development of online transactions, and many other objects and people, momentarily together comprised the conditions for the creation of the security specialist.

As the components of that network developed (for example the security product industry) or mutated (the altered motivations of hackers and malware creators), the interrelations between them have shifted. Therefore it is somewhat facile to attribute the emergence of the field to an event or set of events. It is more useful to describe the components to the network and their associations, as was done previously for the profession and its professional and regulatory context. The analysis therefore moves on to observe how the practitioner relates to their colleagues in the contemporary bureaucratic enterprise.

5.6.3 Enterprise Organogram

Interviewees were asked to describe where in the organisation they felt that the security function should report. This was partially to gauge what level of seniority was appropriate to the role being investigated, but also to elicit whether instinctively the sample believed that security belonged within IT. The answer was near-unanimous across sectors that the function should report to board-level senior management; the consensus was that this level of access was absolutely required to achieve access to implementation authority.

“I would say the highest person for Information Security should report to someone who sits probably at exec level, because you need to have that kind of weight behind you sometimes to make sure that things are implemented.”

[COM73E-AN44]

The feeling was that generally the CISO would struggle to justify placement at the very highest hierarchical levels on merit, but (strongly aligned with the literature reviewed in section 2.2.5) depended very heavily on management firepower to get their policy and message adopted in the organisation. This reinforces that management is a significant actant in the network. Ultimately of course the CISO could aim to join the senior management team itself, although there was less support for this despite the “C”-level title. It is apparent from the remarks of the government interviewee that this was rarely the case and that this undervalued the role. It can be inferred then that government values the role of CISO more highly than their current employers. This is

perhaps a sign that they might in time be open to actions to elevate that status.

“I don't think the CISO sits on the board anyway. There's very few companies who have a CISO on the board *and I think that just reflects where information risk sits within organisations.*”

[GOV01E-GV01, emphasis added]

As was noted in the literature review, it is common to suggest that there is a conflict of interest between the CISO and the CIO and that the former should not report to the latter. Whilst in overall agreement with this view, the sample was less definite on this point than on the question of seniority. The orthodoxy was certainly heard from many practitioners, for example:

“I don't think it can sit in IT because so many of the controls you'll use will be technology-related because it's typically technology that you deliver information through.”

[ENT22E-SM03]

There was a significant minority who felt that either of these issues could be overcome and the coherence of a unified IT-related structure was useful.

“If you find issues within the IT department you have a risk there that they don't get addressed properly ... but on the other hand if you want to get something done, sometimes because you're in that department, networking and all that kind of stuff can help to get things done more easily”

[TRN74E-SM47]

5.6.4 Intra-Professional Stratification

This category reflects the role of technology in security management. From the practitioners, government and professional associations, the answer was overwhelming. This group saw Information Security as distinct from what might be termed “IT Security”, the latter being the *implementation of Information Security policy by technical controls*, such as firewalls, encryption systems and similar technology.

Particularly relevant to this study was the extent to which this separation was seen as both a difference in *content* and in *approach* or *skill set*. With regards to the first, this was both in terms of “professional knowledge base” and the actual scope of work. Information Security was seen to be the protection of the information in any form against any threat. Whilst the storage medium was often technologically-based and hence the attack vector often based on technical approaches, this was considered only to be a subset of the role.

“Information Security covers IT controls, manual controls, physical controls, logical controls. IT Security covers IT. ... It's not really interested in those kinds of things, segregation of duties between manual processes, which are critical. ... I would say IT

Security is part of Information Security.”

[FIN91E-SM15]

Importantly, this view was shared by the government interviewee, something which would be vital to gaining support for a clearly-defined separate profession from IT.

“It isn't just about computers, there's a huge amount of people involved in it as well. I think organisations that focus on the technology will miss the point. Having it in organisations that just do engineering, just do computers, it's not the broad church it needs to be.”

[GOV01E-GV01]

Particularly interesting here was the theme of movement in time. One interviewee described an early security role in very different terms to the modern understanding:

“In [a retailer] at that time security administration was a role that existed, so there was what they would call a security manager at that time. He was more, or completely, operational. ... In terms of ... how would our risk appetite be fulfilled by introducing a particular technology or how wouldn't it be and what were the risks of doing that, there was no knowledge in there at all”

[MIN48E-SM22]

Another contributor suggested a surprisingly short timescale for this movement:

“You know, if you'd asked me twelve months ago, I would have said [that Information Security is part of IT]. Now I increasingly think ‘no’. ... Five years ago I think it was a much more technically-orientated, security-focused role.”

[FIN31E-AN72]

It is not clear that these new socially-informed roles are concrete and stable, since there is little evidence of a closed network and *mobilised* practitioners, however from this data a movement towards an industry more grounded in human factors can be seen. This matches the reported more onerous regulatory burden and evolving mixed threat environment which requires a more mature and organised security team. Therefore, instead of a security component to the technical mix supporting the company IT, Information Security moved to present the board with the ability to control IT on their behalf for security matters, almost switching places in the network.

“I think it's still coalescing as to how this is all going to work for me, but certainly in my head at the moment I see it as a natural move out into some governance”

[CHA31-SM07]

The case of Edward Snowden was noted as an example of a case where technical controls were not seen as paramount. The authorised internal user typically is not only not the target of many control measures, they are also capable of deliberately circumventing them. When the threat moves outside the technical sphere, mitigation options rapidly become less tolerable (since it is

much more difficult ethically and legally to constrain people than to constrain data flows).

“People who use computers are the important thing; they cannot be programmed, you can't put anti-virus on a person.”

[PRO29E-PO42]

Problematisation therefore begins again, since the technical team has no way to offer a passageway to security on its own and must seek a partner who is offering an understanding of human factors. The example was given of closing access after an employee had given notice, causing the employee to simply ensure that all exfiltration and abuse had been completed prior to giving notice. The challenge at this point becomes ensuring that such human issues were raised as important and hence business time spent on ensuring their success. In the wider sense indeed, this position of security near the top of the agenda was seen to be more critical than the technical play.

“The technology challenge wasn't really a huge problem, it was more about getting the buy-in to say these are important aspects that need to be considered.”

[MIN48E-SM22]

It is interesting that there is talk of distinction between technical and non-technical roles almost to the point of dichotomy. The people in an organisation with responsibility for technical security were spoken of in a very separate manner.

“I think there's two types of security people, it's the technical and the non-technical; not completely non-technical but people who are more towards the project governance or security risk management for example or policies and procedures, that kind of area ... [Y]ou have IT Security people and you have Information Security people.”

[COM73E-AN44]

“You're going to put a firewall in of course but let's think about first of all what you're trying to protect, why are you trying to protect it. No is the answer, the simple answer is no, it's a separate discipline.”

[ENT22E-SM03]

This is surprising as most of these people *were* originally technical IT staff. Is this area particularly ripe to be affected by changing training routes in the profession's supply line? If it is true that security managers and technical staff are separating – and this is of course a theme from literature and one of the primary rationales for conducting the study – then this directly supports an attack on the black box of “Information Security professional”, whose unity of role as was discussed above is central to a claim of an independent profession.

Certainly any assumption that there is a single career through which one might linearly flow, from firewall administrator novice to CISO Grand Master is highly questionable. There was a

considerable body of data which suggested that primarily technical and primarily non-technical paths diverged at some point mid-career if not earlier.

But for one speciality to graduate to another is not the only option for both to have status. Anaesthetists for example do not generally yearn to become general practitioners. The sociology of the professions has much to say on the topic of hierarchy; not just between strata of a single profession but between professions and those spun off below. In the same way that medicine sought to avoid tarnishing the ethereal physician with the mundanity of physiotherapy without losing control over the ground, the competent firewall professional can be governed by the security manager without compromising the status of either, provided both have a place in the network and a well-forged link.

“People recognise also I think the value of nursing alongside the value of doctors, and although one would argue that maybe nursing is junior to doctors people would see them both as having a very relevant position.”

[PRO41E-PO86]

The data here suggests that technical professionals did not necessarily view management (meaning security governance rather than mere hierarchical management) as being a career goal. As the security manager is exposed to the realities of business politics, they make a useful shield from that environment for those whose strengths lie elsewhere. Space needs to be left in the network for a symbiosis between those with the technical skills but no desire to lobby, and those content to seek the higher rewards and wider engagement of management but avoid the rigours of maintaining technical expertise (who thus require the advice and support of the specialists). Whilst many people develop both technical and social skill-sets and could move to a security management track should they wish, the feeling was that in many cases the mindset of an outright technical expert clashed with that required to undertake management tasks.

“I think there's quite a divide sometimes. I've got a guy who works for me ... If I said to him, could you stand up in front of twenty people, even people from our own office and talk about something, that would be the last thing he'd want to do. He'd be quite happy about providing the information for someone else to do it.”

[MAN61E-SM05]

For such people the security manager is a source of technology budget and policies which require technical controls. They lobby boards for the money to carry out what the security-aware staff collectively desire, viz. the implementation of security policies (which will include technical controls, and thus employment). Some compromise is needed on autonomy, but in exchange for isolation from the very social factors which are otherwise a threat to the harmony of the old network. Both become passage points for each other, as shown in Fig. 21.

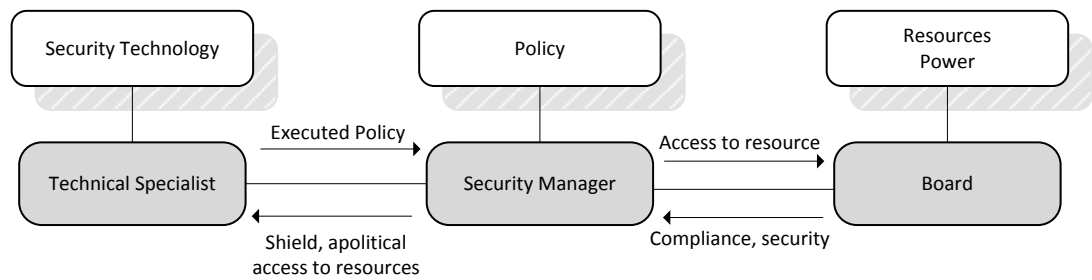


Fig. 21: Potentially peer-symbiotic relationship between security manager and technician.

The distance must not be too great, however. The manager who is technically ignorant must rely on competent advice, causing them to seek a technical expert who is the OPP to that advice. This weakens the position of the manager to politician and quasi-lawyer; they are no longer the OPP to a secure state themselves, they become the person who coordinates the technical responses required by the operational, statutory and regulatory environment. The literature shows that policies which cannot be technically enforced are useless. The manager's position if coming from *complete* ignorance could be easily upset by being undermined by being gainsaid by the technical professional. Such a role of "policy and regulatory specialist" would be valid, but it is much less powerful when a direct peer of the technical specialist. Similarly, one whose governance environment was seen to be overly controlling or unnecessarily arduous is likely to be challenged. In reality, the skills dichotomy is relative; the disgruntled technical professional with political skills would be a powerful enemy to the manager should the relationship break down.

"I think a lot comes down to organisational politics, really. In some companies the technical people can bulldoze their way into getting their way and in other companies they can't, so I think it varies by company and by how much power the different points of view are able to project."

[TEC72E-AN91]

Therefore to this sample, whilst IT is only seen as a subset of the task, governance professionals were expected to be sufficiently versed in the realm of technical controls to be able to relate risk strategy to selection of controls and mitigation actions. For several this meant a period working with the technology was at least desirable, since it was felt to be easier to assimilate human aspects with a technical background than to add technical concepts to governance.

"The skill sets have moved on and changed a lot, but it's worth saying that having the technical background ... makes understanding why and how things can go wrong a damn sight easier."

[MIN48E-SM22]

The overall picture therefore involves a governance professional who has sufficient knowledge

in both technical and policy areas to oversee and govern both competently. This requires a range of skills from some more obviously technical-legal such as forensics (Stahl, 2006), to “softer” aspects such as user education.

“A properly equipped Information Security team should be multi-disciplinary; it should have technical people, it should have people who understand the human element.”

[CHA31-SM07]

The following sections examine more closely the relationship between the manager, the business and the internal client.

5.6.5 Perception and Management

The network around data protection is not simply shifting around “company data” itself, but rather that concept is itself breaking down. This is a result of technical change and an example of the necessity of symmetric treatment of the human and non-human in ANT. Latour (1999b) noted that a gun and a man do not of themselves constitute the same pregnant potential as a gunman. In the same manner, company information processed in manual ledgers is as valuable and nearly identical to the same data stored on a computer, however the possibilities for breaching the security of that data on a computer are different. The combination of data, the storage medium, the access medium, the state of technical and procedural security controls and of the methods to defeat them, the motivations of those who would attempt that defeat and many other factors are not static but form a temporary lattice renegotiated with every change in each.

“Actually to me the question you're asking is, ‘Who owns the data?’ And this is a debate that I've seen in a number of companies, because traditionally IT was seen to own the data, therefore it was up to IT to secure the servers ... Obviously that is IT's function, to have those technical controls, but actually my view is the data's owned by the business.”

[TEC72E-AN91]

There were signs here of a *Business Ownership, IT Custodian* model of responsibility. This moves security clearly to a role as mediator and specialist, responsible not merely for ensuring the safety of the electronics from within but for the safety of the information from without. That suggests the migration across the organogram promised by Neal (2008) and with it the partial liberation from a prior career in system administration, but also brings the assault on the black box of “Information Security professional”, still very clearly linked with the operation of computers. As however the study considers the network today, where this tension has not yet been somehow usefully resolved and the security professional exists in a hybrid state, how they are regarded in their work environment is highly relevant.

Distance from the grubby business of operating firewalls may have advantages, however those

firewalls must be in some way supervised and brought within the sphere of the security professional, to ensure a coherent and comprehensive claim to knowledge. As externals to the business processes and – eventually, possibly – the technology of execution, the security professional must influence from afar. Power in hierarchies is complex, particularly in today's matrix environment. The organisation seeks ultimately to preserve its resources thus they are only usually spent in search of reward or reduction of risk.

“Everything is always for the business. If it has an impact on the running of the business then fine, if that's the way we need to do it then we'll have to do it. Just so long as it doesn't have a detrimental effect on the business.”

[TEC11S-ID48]

As seen both from the literature and the data here, that relationship changes over time as the pressures of easy process and extra margin compete with memories of last month's now-forgotten crisis, therefore stability ideally requires a relatively unchanging external factor such as regulation for its crux. Outside such direct coercive action, the security team must accept that by placing themselves in the position of consultant on processes rather than the experts on technology, they lose the ability to instruct upwards.

“The conversation has to be a dialogue, it has to be ‘OK, well if you don't do this then this might happen, are you prepared to accept that? If yes then fine, but you sign that risk off. If no, here's what I recommend you achieve in terms of outcomes by tweaking your business process. If I can help you achieve those outcomes then please engage me and I will help you’, not ‘You must do this, this, this and this’.”

[CHA33M-SM54]

There are voices here which are much more business-centred than might have been expected in previous years. The practitioners were very clear that the business had to be able to make the decision based on their advice, but that as security professionals rather than operational managers they were neither qualified nor able to insist on their own choices. As above, the danger is that one's position may be untenable if one's advice becomes routinely ignored (or in network terms “ignorable”, i.e. not obligatory). As noted from literature, the question arises of whether risks can be accurately judged by non-specialists, and in absolute terms even by specialists.

“Social media is a typical example of that – I'm using Facebook because I like it, so I tend to over-weight the benefits that social media gives against the risk. This is a typical misperception of risk. Security professionals can be victims as well; imagine somebody who's not educated enough or doesn't know a lot of security, how easy it is. So security awareness I think is the first thing we need to look at before we create a baseline for security certifications.”

[EDU54E-CL11]

The discussion here appears to be in the realm of judgement rather than calculation. The job of

the security professional is seen to be that of two-fold translation. Firstly they must translate the business environment and its risk tolerance into a security policy, and secondly translate the threat in non-technical terms for management for contextual understanding. Whilst the practitioners therefore state that they are providing advice, clearly the rather loose connection between risk, occurrence and outcome allows (acknowledged) room for coercion through the famous “fear, uncertainty and doubt”.

Wishing not to “cry wolf” (and perhaps even putting cynicism aside and allowing a little non-parochial intent) the security manager is required to live in the business. For the management to trust the security function (and hence allow its OPP to be continually renewed), there must be a demonstration of understanding for business processes. That OPP is not absolute and the network rarely irreversible; with a balance of risks it may be that the security action can be bypassed if it itself is a risk to productivity. In non-ANT terms, security is in itself only a means to an end (the reduction of risk and hence loss); if it generates excessive loss (cost) itself then clearly it becomes self-defeating.

“Sitting in the ivory tower and throwing out diktats is something that's reduced the credibility of the security profession in the past, because the business doesn't run for the benefit of the security manager, the security manager runs for the benefit of the business!”

[CHA33M-SM54]

It may well be however that the security manager in addition to being unable to make silo-based decisions through lack of corporate power may be unqualified to do so for lack of impact data. Just as management must understand their risk in context and thus require expert security input, the impact of a problem can similarly only be determined by the process owner who can put the unavailability or corruption of a system in its organisational context. Whilst ANT may suggest looking for a translation of one actor's interests into action by others, this exchange is far more symbiotic; both sides of the risk-reward balance are weighed by their own expert contribution.

So much is not particularly controversial, however nonetheless the change is notable. There is evidence that the practitioners at least are *moving* towards this ideal and thus the situation is dynamic.

“I think in five years' time you're going to get much more commercially savvy security guys because actually all the [technology] is all in place and works. I think we're in a sort of transitional journey to a security world which understands business problems as opposed to understands technology problems.”

[FIN31E-AN72]

In particular, one change visible from the engagement with the user community and hence

seeing personally the impact of security decisions in context is the increased self-awareness with regards to what might be termed *obstructive conservatism*. From the data can be seen that security functions developed a reputation for saying “no” to requests and hence being perceived as blocking, to the point of users deliberately sidestepping security decisions to avoid being obstructed. But far more interesting is the language of self-awareness and intent to avoid this mistake in the future: a clear sign of change.

This is significant since changes towards business engagement require new sets of skills, not always matched by older courses taught by some of the less progressive computer science lecturers shaping the next generation of entrants. Rather than being selected or driven inside an organisation into a new area, these are often expert career technical security staff, sometimes with less experience of commercial practice.

Where then for the specialist adviser? The data from many of the practitioners suggests an outward-facing intermediary, who represents themselves as the OPP for advice which is needed to safeguard the data of the business. The government view was (reluctantly) more in line with the position of the less reactive universities, that security still belongs in practice to the realm of computing, but clearly not supportive of the *status quo*.

“And actually you see that today, when you talk to large organisations about their information risk they largely point at the CTO and the IT department and say, ‘That’s their problem,’ and that’s not the answer.”

[GOV01E-GV01]

It appears then that this change is happening within businesses and that there is an intrinsic lag between this reality of practice and the reactive mechanisms for teaching and monitoring it.

5.6.6 Users and Culture

It was uncontroversial that user education was of paramount importance for the modern security organisation, across all types of interviewee. It was particularly interesting to see strong agreement to this from education; one interviewee strongly believed this supported risk management decisions being taken from an informed standpoint. This is also seen as key for users who are able to cause damage through error, ignorance or misjudgement. Whilst this was strongly advanced, it is highly aligned with the literature and thus not useful to note further in itself.

More relevant is the rationale and language used by the practitioners who are attempting to enrol their workforce. Again, it is perhaps a truism to say that security depends on informed users avoiding incidents. Most interestingly for the ANT study is that this set of interactions is

seen to be the weakest part of the network, and one of the most significant. For example, the juxtaposition of large amounts of data and near-instantaneous mechanisms for distributing it creates a risk, which has apparently proven difficult (or unpopular) to mitigate technically. Neither Data Loss Prevention tools nor other technical means of constraint were mentioned positively in terms of the risk discussion.

“If I were to implement a really, really locked-down security policy across all these different systems I would probably be put into a bag and thrown into the canal!”

[TEC11S-ID48]

Pragmatically then, although the security officer might wish not to have technology usage choices in the hands of a fallible person who is able to make their own policy decisions, it is recognised that this is the case and thus an educated user is better than an ignorant one. But they must be enrolled despite fierce competition. As was noted in the literature review, the user’s primary concern is completing their own work to their own priorities and thus by default security concerns will not be paramount. This theme was seen also strongly in the data.

“If someone’s particular job is to get some code done by a particular time, that’s what their bonus is tied to, that’s what the project manager is stressing them about.”

[FIN22E-AN43]

In ANT terms this is classic enrolment permanently in play, due to two competing interests. Using the above example, superficially we can see this as project manager and security manager both competing to achieve that enrolment, with differing devices of *interessement*. The security manager is looking to enrol the user base, to act powerfully as scouts in the enterprise and to ensure adherence to security-preferred policy and practice. Seen from another angle they are the OPP to an implemented policy for the security manager. The security manager however must themselves present a case for the employee. Where the function is strong (due to successful enrolment of the board to obtain “teeth”), waving the threat of non-compliance sanctions is strong motivation even against competing offers. From the language of this sample however, in their experience this is often not the case and the employee has a substantial counter offer internally from those looking to achieve delivery of some other activity. This need not be a financial bonus of course, simply a more realistic prospect of sanction from another side, perhaps line management, reputation or career progression. This adds further data to that of the survey-based studies of policy compliance.

But perhaps this dilemma for the employee can be at least partially resolved by socialised security. The account has not yet mentioned general corporate health and success, which are fundamental to the goals of *all* actors. An appeal can thus be made to all internals to ensure that they understand the reasoning and justification for the action. This moves the security manager

away from competition for the “employee” actor’s effort and an OPP towards a stable foundation for business operations. Moreover, the antagonism and competition described above are drawn from the orthodox concept of security being perceived as incompatible with efficient business practice. Actually the data showed clear alignment with light-touch security if at all possible.

"If somebody has caused a security incident by bypassing a security control that actually impacted their productivity so heavily that the only way to get their job done was to go around it then that security control was poorly designed and poorly implemented and it's not the user's fault."

[CHA33M-SM54]

This then is the upshot of that negotiation around problematisation. The security manager has had to learn to respect the business process and the user. This “Users are not the enemy” concept (Adams and Sasse, 1999) is not new, however the language used in this data is mostly pragmatic; autocratic and distant approaches are seen as not *effective*. Where users must take risk decisions, they must understand the concept and they must understand the risk.

“I’ve always believed that the first action should be to increase investment in security awareness programmes ... because security in my view is more like a philosophy rather than a profession. ... I do honestly believe that security awareness is one of the most important things and we need to train, even cyber security professionals, on how to stop misinterpreting risk.”

[EDU54E-CL11]

How then is this training performed? One very strong theme was the requirement to put the information in the users’ own language. Whilst there were references to the usual aspects of marketing a message (a skill in its own right), the predominant theme was translating a technical concept and putting oneself into the mind of the user, as reviewed in section 2.2.3.

“I think some technical people are very much capable of doing a non-technical role but I think the majority of IT professionals might have difficulty in explaining technical stuff in non-technical terms.”

[COM73E-AN44]

This empathy requirement appears to represent a skill fault-line in the profession; a *shibboleth* for informed modern practice. Whilst tolerance for technical ineptitude may become less necessary if workforces become “natively” proficient, the requirement to explain security-specific technical concepts seems more permanent. It appears common to use personal-use training as a way to sell awareness information:

“‘Let’s help you understand how to secure your computer at home and your smartphone and your tablet’ because that interests people more than hearing that they need to be careful with this month’s figures for France, or something.”

One might posit that this is the use of information as a lure for enrolment, such that a person so trained is unwittingly mobilised into action on behalf of the security team. In a sense, the personal tablet can even be seen as an actant here, since it has become a passageway to modern social life and driven a change in user behaviour such that IT managers seem to feel powerless to resist functionality demands which are not essential for work processes.

Another fascinating code was how security belonged to every role, which supported two concepts. One of these was entirely predictable: that it is the responsibility of all to contribute to the general security effort. Shorn of the security references, this data could equally apply to Health and Safety. It is not however frequently suggested that *because* of that universal responsibility, Health and Safety is not intrinsically a specialist undertaking. The second concept *did* suggest this for Information Security however, from surprising quarters. Perhaps the most striking element to emerge from the government interview was their representative's reluctance to embrace security as a speciality of study. The preference here was very strongly for graduate (software) engineers to be trained in security (begging the question *by whom* if it is not a speciality), and thus betraying an implicit assumption that Information Security is primarily a question of avoiding computing platform vulnerabilities.

“Again you see, if you've got engineering right then you don't necessarily need security so much. Or if you got some of those other professions right you don't need security.”

[GOV01E-GV01]

Placed with similar comments from within a major professional body for computer security, this is very significant. In themselves these are offhand comments in an interview and not completely thought-through statements of policy, thus it should not be over-analysed for content. What this shows is that whilst they may have socialised positions on many topics, people in influential positions in the professionalisation project of Information Security interviewed here have a fundamentally computer-centric viewpoint, and are themselves in a state of transition from one state to another. This will be explored further in the next chapter.

5.7 Summary

This chapter presented those parts of the data which were noted strongly in the analysis, either due to the frequency of coding of that concept or due to an analytical memo created during the various stages of the transcription and coding process. These have been used to suggest fragments of the overall Actor–Network at play, and in particular where that network is incomplete, in flux or under tension.

This study's research questions concern the origin, current status and future prospects of the Information Security profession. Addressing the first of these, Section 5.3 outlined the emergence of Information Security roles over the past few decades, noting the profession's relatively fast rise and a range of events and factors which the interviewees felt were contributory to this. By describing the contemporary network, it was possible to show that changes to the regulatory and technical environment created a specialised area of knowledge and practice, and hence the possibility of a intermediary role between management and IT. How that position has developed into a variety of modern specialities was addressed in section 5.4; in the following chapter this will be developed further to examine roles in the profession in detail to address in particular the second question of current status. Section 5.6 also contributed heavily to answering this question, firstly by drawing out the relationships between technical and human factors in modern practice as seen in the data, and secondly by describing how current practitioners are viewed and ranked amongst workers in their employing institutions.

Answering the third question of future prospects depends heavily on the issue of training and qualification. In section 5.4, views on certification were discussed, showing the early requirements for a practice-based qualification to act as a guide for recruiters when personal recommendation became impractical. Whilst voluntary professional certification was not unwelcome, the primacy of experience was stressed over qualification. Within the sphere of qualifications themselves, university- and practice-based qualifications were compared, noting no sense of competition. The following chapter will show how, by contrasting the current model of entry, training, education and qualification with that of more established professions, we can predict a shift in future patterns. Similarly in Section 5.5, by comparing the attitudes of practitioners and government to licensing differences were seen between traditional models of professionalisation and that being followed by the present profession, alongside how the very concept of profession was regarded by the interviewees. How these themes interrelate will be examined shortly.

In the following chapter the major themes which arose from this data are drawn together for further discussion and developed to form individual conclusions. Each touches on aspects from all of the strands of enquiry established from the literature review, therefore in the final chapter these conclusions are finally juxtaposed with the individual research questions to bring the work to a close.

Chapter 6: Secondary Analysis

In Chapter 5, founder members of Information Security describe working in a new but diffusely-bounded area of knowledge bordering several established fields. The causes suggested as contributory to its creation—both technical and social—were several, pointing to an *assemblage*, or momentary confluence of factors. These early workers described admission and advancement as by peer recognition, however growth forced this to give way to scalable and objective testing. Testing required the establishment of certification [professional] bodies to provide a rudimentary independent guarantee of competence to assure HR departments and managers, alongside giving the holder much-needed confidence.

For this purpose, they were seen to be effective enough. The profession however should then have entered a long period of consolidation, according to theory, where specialities were established and qualification routes created. Over time, these should have experienced Abbotonian competition for jurisdiction over discrete areas of new knowledge; ideally, a hierarchy of fixed roles would have emerged, perhaps similar to that of medicine and law. Ultimately, the unified profession would have approached a sceptical state for permission to regulate itself and control entry.

The data shows that this has not happened. The same network which created the conditions for the profession's creation has developed so quickly that its development cannot occur quickly enough naturally, requiring catalysis. The certification bodies are still trying to gain legitimacy and perfect their credentials within the model shown in Figs. 16 and 17, which requires a “graduate profession” status that was not supported in this data. Government, suddenly aware of a grave threat and forced to take up this unrequested role by default, is therefore raising the status of an occupation which it feels is losing out to more established professions. Professional status however was not found to be a priority for those who are already in employment and wish not to be displaced from it, certainly not by something originating from a government whom they do not trust. Meanwhile within industry, practitioners report still having continually to re-win resources and authority which might challenge operational efficiency, and thus have had to become operations- and human-centric risk managers.

Expanding on these findings from the initial analysis, this chapter goes on to describe the development and current state of the network in more detail, presented within the major overarching themes which emerged during the execution of the analysis and based on observations and annotations made throughout the study. For each theme the principal arguments arising from the analysis are advanced, leading to their conclusions. Throughout these will be related back to the topics of the project's three research questions: *origin, current*

status and future prospects.

Section 6.1 principally concerns the first question, describing the origins of the profession as identified in this data. Thereafter the chapter turns to the questions of current status and future prospects. It is considered whether the network surrounding Information Security practice has reached the point of irreversible translation (all actors have defined roles which they accept, have been enrolled and mobilised into action) or whether barriers to this state remain. In section 6.2 the “Information Security professional” actant itself is examined to establish whether it is well-defined and stable with recognisable roles. In section 6.3 the process by which practitioners are educated and trained is discussed, to further observe the homogeneity of the occupation’s professional identity amongst entrants and those who teach them. In 6.4 this new candidate is compared with idealised concepts of *profession*, the current workforce’s degree of intent in its movement towards professional status is discussed, and the topic of licensing is considered. Finally, in section 6.5 the chapter is summarised.

6.1 The State and Stability of the Current Network

As stated above, the first research question concerns the origins of the Information Security profession. If it *is* a profession then it is a new profession; to explain its current position requires the analyst not simply to identify this new actor but to describe its task and genesis. The more established interviewees of all types have observed the emergence of security within their own careers. Management was eventually convinced that there was a threat (during problematisation), but maintained its existing links with the IT department which had established itself as the OPP for computing matters.

This network surrounding IT and audit in the workplace was affected by the new actor, whose emergence created tension around those established relationships. The literature notes that increasing technology complexity creates more opportunities to perform services and hence interest others in those services. Security however was different, in that the new actors faced particular challenges to achieving network change. Whilst expanding technology capability created further specialist IT roles to be added to the existing environment (without threatening it), Information Security had *contrary priorities* to the existing settled players and thus, initially, to those of their potential clients.

Where previously technologists had offered themselves as OPP for computing functionality and performance, security pushed for constraint, cost and control, to resist malign actors whose presence was only initially felt by the technologists. The new actor had to both prove first that their services were useful and desirable (to people hungry for performance and largely unaware

of threats) *as well as* the usual demonstration of competence, in order to establish themselves as OPP for that service. Since enterprise policies require changes to behaviour they required sufficient powerful buy-in to resist heavily-entrenched and established network links which were being continually re-made in the course of daily business. It is not surprising therefore that it required a number of events in order to make the prize worth the cost required by its OPP, the Information Security professional, at least outside the military.

To see the rise of the occupation as a successful campaign by the new internal actors is to overplay intentionality. The real force here came from both technological change and human actors which inhabited the threat landscape. Technology forced choice, mobility and responsibility into the hands of the human user, in turn forcing human behaviour and culture into the realm of securing computer data. Therefore this should not be described purely as a new profession in the Abbott sense, since a criticism of Abbott is that he presents no mechanism for concerted action of an as-yet unorganised set of people (Macdonald, 2005). To see the new space emerge for IS practice is to see the continuous fracture and development of a network over several decades. The new profession might have had intent, but its success is also a response to those actors whose interests were catalysed by technical change.

Looking to that campaign to enter the network, a starting point for the study must be chosen. Security itself has deep roots but wartime encryption is the most prominent recent cited example of technical progress enabling the protection of or attack on encoded information. One of the more experienced interviewees listed it as a foundational topic in the new arena of computing security.

Yet early networks which included security were not stable. The literature notes that several stages of maturity were required to move from technical reaction through to structured governance and systematic proactivity. The early spokesmen for the network security technicians who presented their trade as OPP for a secure state failed, partially because they asymmetrically addressed the threats from the machine and its human operator, underplaying the latter. But when the first major viruses easily outgunned the technical solutions ranged against them, it was the complicity of the untrained internal user which facilitated the realisation of the threat. Thus whilst considerable ground had been made bringing security forward as a topic, the occupation with purely technical computing spokesmen could not become stable whilst the human and governance aspects were excluded, as they could not genuinely deliver what their management required. A new class of worker – a new actor in its own right, able to understand the technical context but also able to embrace social, legal and behavioural aspects – was required to allow the network to accept a new OPP.

Why then was there a delay to the creation of a stable network? The caricature above makes two errors: firstly assuming a highly simplistic binary world of “secure” and “not secure” and secondly to assume that business managers can distinguish between these accurately. The successful translation of the new actor’s offer into an established OPP is a more nuanced combination of developments. Several interviewees recall early commercial Information Security as almost non-existent, with little progress in some places until surprisingly recently. As the topic grew in prominence, associations based on mutual interest eventually formed, with recruitment into the few early roles reported to be primarily by personal recommendation.

The range of events to which expansion in security focus was ascribed (amongst them the expansion of the Internet in the early 1990s, key mail-borne viruses from later in that decade, data protection legislation, standards, the development of online commerce and others) was sufficiently wide to suggest that in fact no single technical development was completely instrumental. It seems more likely that with each development *such as* each of these, the pressure to secure the computing environment increased gradually and the cost of effectively acting maliciously decreased. There was a range of threat vectors, from which a subset might affect the network in a particular context and industry, albeit with many areas of commonality. In response to one of the research questions then, the motivation behind the expansion in security awareness was seen not to be linked to one single actor in this data.

One interesting mode of action reported was the initiative taken by those first specialists. In some instances the security department (or educational course) was founded by those initial acolytes who agitated for change in their local environments, possibly with the “reward” of being asked to undertake the role thereby created. The developing IT-based actor began to experience internal tensions and break down into constituent components of security pathfinder and traditional technician.

Prior to these malicious new threat vectors the early network around Information Security was apparently small. There were few external actors to prompt a reaction inside the corporate world, no real mechanisms to propagate external threat into internal action, and even relatively little work undertaken in academia. The network was in a state of limited problematisation, with few people looking for action and few actors starting to offer a passageway to that action. The existence of other professions as a mimetic template, later to be highly relevant, had no contemporary effect. Yet the growth of those external actors was sufficient to cause at least modest recruitment of interested specialists (interviewees describe this). Two professional association interviewees noted that this expansion caused a *problem* for those recruiting (in one case for education, in the other for employment): a test was needed of competence since existing

methods were not scalable. This change of mode would have acted to force change on the network and hence the nature of the profession. It is this *change* which has the most significant potential for development.

With advancement no longer in the gift of an individual (with all the social interactions implied in securing the good offices of another), the route for entry to the profession would surely have changed around the new “certificate” device and allowed a wider set of people to gain entry or recommendation. Recruitment for advertised roles was no longer limited to those around the personal web of people looking to drive and develop the topic through association; scope existed for people who wished purely to practise without close links to the association of “fathers”. An actor had stepped in as spokesman for the profession and issued a device of *interessement*. The fact that multiple claims were made with differing approaches however shows that none was the clear OPP to a settled single profession at that point.

Armed with a certificate device, the “professional” actor now derived claims to status and competence not purely from experience and good standing but through objective testing. They possessed competence certification in a specialist field issued by an authority body and started therefore to *look* like a profession – which theory states is significant for acceptance as one – bringing the structure of other professions into consideration. But this also created the potential for tension between those in the industry with the certification and those without, particularly where there was a difference in experience, and hence weakening of the incomplete foundations of each spokesman.

It appears however that the network instability which supported a new discrete profession was most prominent in business. Whilst professional organisations and practitioners are alive to the modern business context for security, the pace of change has created a problem for those responsible for training the new entrants in the universities. Rapid advancement complicates the filtering of transient fashions and concerns into new discipline-specific knowledge, a concept which only started when vocational university-based training was developed during the professionalisation of Victorian engineering and which was rejected by the older professions as too narrow (Andrews, 2016).

Without a source of deeper, conceptual learning, there is no basis for a graduate profession; academic institutions teach timeless concepts not train current techniques. Neither though does a profession defending against constant technical attack require theorists with no practical skill. Medicine solves this with intercalated clinical coaching and anatomical learning; law, with post-graduate professional pupillage. Government by contrast needs an immediate army of ready-made security staff. Having established then the origins of this profession and thus addressed

the first of the research questions, the rest of the chapter moves on to discuss how that profession is currently faring and how it may develop in future.

Starting with its current status, the occupation has moved through a long period of constant change, which has defied the attempts of any one party irreversibly to establish a firm network around its efforts. It is then in a state of *flux*, constantly looking to establish a new network containing one or more well-defined OPPs for aspects of its product (security), whether that be the genuine protection of information or simply compliance with some external compulsion.

It exists in an environment which is not so much artificial as expanding at a challenging speed. The sheer pace of technological change and the increasing threat of sophisticated criminal and state players has altered its arena and identity far more quickly than most threats to human health or wealth evolved. Methods of recruitment have thus been transformed from non-existent through mutual personal recognition by peers to large-scale testing *within a generation*.

“Security is such a fast-moving feast, I don't think there's anyone that knows everything there is to know about security”

[EDU45E-CL31]

Given the growth of specialist degrees, today's entrants are becoming vocational apprentices, no longer accidental converts. This workforce increasingly enters directly after theoretical preparation, rather than transferring from an IT or auditing career. At the very least they are entering a more mature field. As ANT insists on viewing networks not as fixed relationships but as bonds made durable by being reaffirmed constantly; such large changes in the character of that actor's constituents must *surely* challenge the reproducibility of links which were formerly made by others with different intentions and backgrounds.

What changes will result from this? Those who chose a vocational career are possibly more likely to associate with their kind more strongly than those currently in post who entered in mid-career. This is of course only a generalisation; famously converts in many fields often exhibit greater zeal. However it seems reasonable that those choosing directly to enter a discrete profession actively recognised and promoted by government would be more aligned to its identity than those who have lived in a hybrid and confused, unrecognised state, particularly given that their initial training and identity formation now occurs first and independent of any future employer.

There must also be a world-narrowing effect from losing the “tour of duty” outside the protected sphere of the security team. It seems likely that a security professional who has never been controlled by a security team or undertaken business operations processes might lose some

degree of empathy with later clients. Success for a security department requires the acquisition of power, to have policies obeyed even in the face of operational impact. This is evident from the plaintive tone of practitioners unable to compete with the demands of business process economy; but notable also is the empathy shown at the same time towards their internal clients. Many interviewees understood themselves to be part of a team whose overall goal was for the company to succeed, which fails if security takes a parochial or dictatorial approach to its work.

Where was this learned? There must have been importation of these experiences by those who entered from outside, even though their main provenance was IT rather than business operations; as a principal tension observed in the data was between security manager and technician, this is probably a powerful tool for empathetic training. It seems highly likely therefore that a vocational direct-entry profession with increased status and power will find it harder to ensure continuity of that business-centred approach, and hence their ability to enrol senior management irreversibly is damaged unless this is included in their training.

Conclusions relating to current status:

- It was reported (reinforcing earlier findings in the literature) that practitioners have real influence at management level only during crises and that resources must otherwise be continually re-won, but it was seen here that perpetually referencing problems to gain resources was ineffective due to “crisis fatigue”. This suggests that the network has not yet achieved a state of complete translation and that other, more powerful actors are still competing for the attention of management.
- Professional status in its own right did not emerge as a powerful motivator for the existing professionals. For many the topic was novel and responses hesitant and exploratory, in contrast to other areas where answers were more confident and considered. Current workplace status was seen to be derived from personal reputation rather than simply derived from membership of a chartered profession. In principle the government actor by encouraging professional status to aid recruitment, may be attempting to position the profession as an OPP to a state which is *not actively sought* and hence its attempts to alter the network to its requirements may be unsuccessful.

Conclusions relating to future prospects:

- Conversely as the *next* generation will *choose* to enter this occupation against competing opportunities its status *could* be a relevant factor. It was felt however that Information Security was not yet well-established as a discrete occupation outside its

immediate interface occupations thus this might be of limited effect for school-leavers who have not already been attracted by personal interest and hence already enrolled.

- The network has undergone and is undergoing constant change which has prevented any one form of Information Security professional actor establishing itself in a durable form and hence the network from becoming irreversible. Those currently practising were recruited, socialised, educated and trained differently from those entering today and hence any network translation which forms around their interests is unlikely to remain completely stable when they are replaced by successors with differing interests and experiences.
- Whilst many were wary of comparison to professions which deal with the vital interests of the client, Information Security was felt to have sufficient depth of knowledge and gravitas to become a recognised profession at some future point. The lack of maturity of the profession was strongly cited as a blocker to immediate progress towards acceptance however the occupation was felt to be moving in that direction and this was not unwelcome.

6.2 Roles Within the Profession

When considering the current status of the profession, a key topic is how distinct and well-defined it has become. Unifying the domain was a concern for the IISP (Lacey, 2006) right from its formation. This data shows that the existence of a separate profession with its own identity and body of knowledge is not at all universally accepted, although the controversy is along unexpected lines. From the literature it was seen that Information Security has emerged in large part from IT Security; failure to dissociate itself from here as “parent” to some degree would be predictable. Similarly there is some confusion between jobs, titles and ranks despite the emergence of role frameworks.

Rather less expected was the suggestion that security was not the preserve of specialists but rather was a common property of all areas of practice. According to this line of thought, if programmers, technologists and others considered properly how systems might be abused then there would be no need for a specialism.

“Security in my view is more like a philosophy rather than a profession.”

[EDU54-CL11]

In itself, this is highly unconvincing. Whilst it is possibly true that at a micro-level good security practice minimises vulnerabilities, this does not preclude the study of secure practice itself as a meta-activity. This appears to be a corruption of the adage that security requires everyone’s vigilance, which *is* a valid fundamental. A comparison may perhaps be made between “security is part of every role” and “mathematics underpins every physical science”, and the consequent absurdity of thus deducing the non-existence of pure mathematics. Similarly compliance with law or Health and Safety policies is part of every person’s responsibility but these fields continue to have specialists. In any case, the problematisation in a professionalisation campaign is aimed at providing a passage point to *specialist expertise*, not exclusive access to all aspects of everything touched by the expert domain.

Whether that position is accepted here however is irrelevant, since it exists as a concept in the data. It undermines the position of Information Security as a graduate profession since security concepts are seen to be needed prior to undergraduate level as general life skills. But surely there is a difference between the study of the subject and learning the fruits of it, such as learning healthy eating as a teenager well before going on to learn physiology as a medical student. This way of thinking appears to reduce security to a software engineering quality concern rather than something with its own conceptual learning.

The previous chapter positioned security at the nexus of a web of other actors, particularly in its

business context as OPP to security and compliance for management, whilst its earlier incarnation mainly mitigated technical attacks on computing infrastructure. The advent of remote terminal access erected a convenient professional divide between securing a place and securing a system inside it, attacking the settled network surrounding physical security and supporting a new class of actor. Experts in this technical exercise do not seem to have been exposed directly to senior management, being (however specialised) a member of a technology team. An important niche was created where they could become the passage point for their technical management to comply with the demand for an untroubled IT environment and no consequent reputational damage or regulatory action.

Overwhelming lip-service at the very least was paid to the concept of socially-informed security practice, and much of it was apparently heart-felt. This concept is clearly becoming an accepted part of the shared culture and values of the lived occupation. Security governance was felt to be more naturally at home in the rarefied air of senior management, lobbying for delegated power to impose policies and ultimately sanctions in return for safety and compliance. Some requirement for soft skills is substantive (it comes from the requirement to present and agree policy) and some from pure organisational operation; all departments need resources and need their leaders to be capable politicians in front of the board.

But to present governance as having left its technical roots with IT Security as only one facet of its portfolio is dramatically to overstate the situation. This is particularly true where the apparent level of risk does not justify a dedicated department and high-profile charismatic CISO. This is for two reasons: firstly because boards reportedly still see security as something to be “done” somewhere else and only take notice when things go awry, and secondly because the technical roles are clearly still fundamental and vital.

It is not an essential challenge to professionalism nor to the aspiring security actor for boards to see security as an important issue which must be delegated; indeed this creates the claim for a profession. The Actor–Network requires a security specialist and a buffer role between the political realm and the purely technical realm, the buffer being a potential avenue for the security manager and hence a discrete professional identity.

It does not appear however that there has been a successful campaign yet to establish that profession with the same gravitas as one of the other advisory professions represented either directly or by executive proxy around the board table, i.e. who are present when the bonds of association are re-made by the most powerful actors in an enterprise. The accountants (OPP to legal and effective financial advice) will be represented by a Finance Director. The lawyers (OPP to protection from the vagaries of legislation and lawsuit) are represented by a Legal

Director, General Counsel or someone whose word carries equivalent gravitas because of the importance of their advice. This sample felt that security had not established anything like this degree of influence in the network, outside the *immediate* drama of an incident or urgent new area of compliance, and hence the “professional” status is clearly not fully established. Security is a task to be “done” by someone, managed only by exception and probably represented by IT—a servant to the business, not a master. By contrast, its opposing voices in terms of operational freedom and lack of restraint will be represented by mainline senior management.

The lawyer and accountant however have well-defined and well-established identities referenceable within the network. They are known (inscribed into the network in a way which is not ever doubted or checked) to be positions for which considerable study and qualification is required. There might be an internal hierarchy and internal sub-division between specialties (which is presented as ensuring that the professional skill is at the elite level claimed), however each presents expert advice to be ignored at significant peril.

There has been significant movement towards establishing a similar scheme within information assurance, where SFIA-defined roles⁷ have been linked to government-backed CESG (now NCSC) Cyber Security Professional certifications and training (CESG, 2015; GCHQ, 2016), which in theory would allow the actor to reference the authority of state recognition. The feeling from the interviewees however was that not only was this *scheme* not well known, but the concept of a security specialist *in itself* was unknown outside IT. *However* these newly defined roles inter-relate or rank in terms of skill even if they were well established, the *existence* of the entire occupation was felt to be unrecognised.

Beyond this, the roles laid out by the SFIA do not show an easy mapping to the roles of many of the various security managers and practitioners interviewed. It is not clear how they inter-relate with each other hierarchically outside huge government/Enterprise organisations which can employ all the roles. Moreover, these roles describe a reporting structure within a company but do not define the hierarchy of the professions themselves if there is no technical supervision of one by another. A theatre team may be led by a surgeon but the anaesthetist remains a member of a peer profession to the functional team leader whereas the nurse’s profession is subordinate.

The data collected speaks more of a security function responsible for creating policy and those elsewhere responsible for technically executing it, with the degree of distinction affected by factors such as size, industry and organisational maturity. Security managers establish

⁷ Skills Framework for the Information Age

themselves as the OPP for a secure state but know they cannot personally deliver it; they rely for this on the prowess of the longer-established but possibly less management-facing technical specialists (who may identify with one of the other SFIA roles). In turn this is probably a happy state, since the security manager can also pose as the gateway to those specialists for accessing resources without interacting with business politics.

Looking towards the question of future prospects, for this network to become stable these actors must surely need to become less diffuse and establish themselves clearly and distinctly in an Abbotonian manner. Can a public (for which read adjacent actors which need to be enrolled) really interact with seven or more flavours of a profession they don't even recognise? In turn, does each person in the industry today associate with exactly one of those labels and accept their position in a skill hierarchy based on them? Is there a network established in a security team based on actors claiming these roles and their associated badges? Management need someone to whom security can be delegated, someone who in turn must force them to pay more reliable attention in good times as well as bad.

Completely technical staff require intermediaries as managers, and as they do not universally aspire to management positions or work in non-technical aspects of security these intermediaries are not necessarily of their own kind. Governance-centric security managers with business and social skills able to bridge this gap have begun to emerge and insert themselves into that web by acting as diplomats to each side, however they must displace someone's position in the established corporate network. But the linkages from technician to IT Operations to IT Director to Board are reasonably strong. This new network has the potential to become fixed and stable, however this newcomer intermediary-manager actor has not completely translated their will into a settled hierarchy of professions, merely of business roles. Their own identity, both of itself and how it relates to IT management and staff, is not yet accepted and defined.

Conclusions relating to current status:

- A credible and substantial framework exists to codify a list of roles in very large organisations linked to a reasonably distinct body of knowledge. Despite this, there remain few well-accepted and understood named roles for Information Security workers, particularly outside this scale of organisation, which reflect specialisms within those bodies of knowledge, nor workers whose tasks routinely embrace all of them. This prevents the quick formation of a network of peers, clients and staff within an organisation with established roles based on the claims of professional qualification and role definition which are associated with more established professions. Instead it is

more likely that networks must be formed in each enterprise context around the individual's own ability to interest and enrol their own contacts based on personal attributes and skills, whilst peers in other occupations can make use of an extended network of negotiated and more established relationships by presenting their professional status devices as a primary source of workplace identity and claim to expertise.

- As such, whilst expansion of security knowledge has allowed a new species of professional-type actor to appear which is distinct at least in the workplace from the Information Technologists, it is not clear how that profession is structured internally with regards to hierarchy and form of any sub-categories of professional. Again, when relationships between workers are formed within a particular environment, that network cannot import easily the templates and identities formed by skills frameworks, leaving the individual actor not simply to establish themselves as OPP for a known brand of service on the basis of known standards but instead to do so unaided.
- The principal fault-line for divisions in the data was seen to be the social–technical axis, with uncertain relationships between those who sought to be the OPP to competent technical administration and those whose interface was directly with management. The data suggests distinction between technical workers and security management workers which went beyond normal hierarchical control within teams. Instead it was felt that these were distinct skill sets and that the technical group, whilst equally important and competent, did not aspire to progress to the management group *nor saw it as superior*. A new network where a security manager actor is an OPP to controlled technical skills to management – and resources and a shield from management to technicians – is possible.

Conclusions relating to future prospects:

- It seems likely that rationalisation to a small number of discrete roles with an accepted set of inter-relationships and potentially codified discrete specialities will be needed prior to further professionalisation. At present the network is merely problematising and cannot move on to forming durable links between the actors thus identified based on their various interests. Until the actors can successfully reference and import more recognised and durable identities from a network of larger and more powerful “regulator” bodies their ability to enrol others will be compromised. Either all roles are peers within Information Security and regulated together, or the security officer profession is superior to the others as medicine is to the medical para-professions.

- The practitioners felt on balance that as an OPP to secure practice, which might clash with those seeking to be OPP to technical performance and agility, security governance should form hierarchical relationships directly with senior management outside the IT hierarchy. Furthermore the practice of IT Security was felt to be only a subset of Information Security and hence those actors only able to offer technical competence should take a different place behind security management in the network. This does however require the development of strong business skills and sufficient vision to see security in the context of an effective organisation which is not unreasonably hampered by overly-restrictive rules, otherwise they cease being an OPP to a desirable state and their bonds will be too easily attacked by others appearing to offer lower cost. This will further create incentives to split the profession into a technical enforcement layer and a less technical business-interface or management layer with differing emphases in competences.

6.3 Preparation for Practice

Implicit in the settlement of roles described above will be addressing the crucial question of vocational formation and preparation. The UK Government gave its responsibility to address the security skills shortage in the country as a motivating factor for backing a Skills Framework. Without well-defined roles with set specialist training, it is difficult both to express and to deliver the correct preparation to new recruits and to ensure the correct mix of skills is taught. Whilst individuals might be able to function as actors within a network in a work context, at a national level governments cannot form relationships with thousands of workers and can only interact effectively with spokesmen for an enrolled workforce of identifiable role-holders.

Whilst a detailed review of cybersecurity education is not in scope, vocational preparation is of particular relevance to a study of professionalisation. Aside from the importance placed upon graduate formation in the professionalisation literature, it is a key source of network reversibility. As mentioned, those in senior positions in both industry and academia (such as were interviewed here) had little opportunity to develop a security-based vocation prior to entry. Any such vocation would likely have been expressed via a career first in computing, via its established academic or non-academic routes.

It is significant that few interviewees considered security practice to be unequivocally a graduate role; to contrast this with law lecturers, the legal regulators and practising solicitors, would show a far more powerful and harmonised statement of the essential nature of graduate pre-qualification. Is this then a failure to professionalise, or a failure of the orthodox concept of professionalism in a modern profession? In reality it is a reflection of failure to *define*. With actors forced to adopt individually-negotiated roles in workplace interaction, there is an unordered spectrum of potential roles possible and routes to competence therein.

The previous chapter showed that universities exist in a market for entrants (quality of entrant matched *ceteris paribus* to prestige of institution), delivering employability in exchange for fees. The university aims to be a passage point to an academic degree and must enrol the best students it can recruit. This comes at a cost to the student, and when graduate status is not mandatory, passage through university cannot be obligatory. This said, where there is evidence that graduate status will be highly useful in later career then much traction can be gained during *interessement*; the degree certificate is still a highly prized product in the market.

The regulation of degrees by government to improve the pipeline of workers suggests that it expects – despite saying in interview that graduate status is not *necessary* – to hire extensively in the graduate employment market. Information Security supports extensive conceptual

learning, as evidenced by its validated undergraduate programmes; why then a reluctance to specify graduation as a criterion for entry?

It seems that this flows from lack of structure. If one were to ask whether all NHS workers required graduate training, the answer would surely be negative. Medicine having devolved patient care to subordinate roles, it is possible to establish that, for example, auxiliary nursing does not require graduate preparation, that registered nursing does to bachelor level and physician to doctoral level. By establishing these lines and their inter-relationship, the nursing authorities as spokesman can exert control over their own training. By controlling access to registration they become OPP to the university, and thus student, for attracting professional status and right to practise. Such a codification was seen to be missing in this regard for establishing the boundaries of the graduate, professional security practitioner and its supporting workers.

Predictably, universities certainly appeared to regard security careers as almost necessarily proceeding from graduate study, whereas neither government nor the practitioners were as convinced. This may further undermine the unity of the security professional role; government, currently supporting doctoral research at a number of centres, nonetheless saw security as having too many constituent roles and too many levels of practice to be an exclusively graduate profession. Its support for inclusion of graduate and postgraduate roles in that spectrum however is very clear as it acknowledged the positives of study first at master's level and now at bachelor's.

To ensure that the profession's common knowledge remains relevant and captured, a feedback mechanism is required between practice and teaching syllabus, and indeed these are being tried. In one case, an interviewee was both academic lecturer and practising consultant, a model very familiar to the medical profession with its eminent researcher-practitioners. In one institution, external speakers were routinely invited to lecture; in another, employers were consulted as to which skills would be most useful to teach. In terms of addressing the study's title question therefore, there *is* a vocational degree system being built with a socialisation process – feedback from practitioners to those in formation is underway.

Furthermore, educators were confident that their courses were suitable and sufficient to place their graduates into an entry-level job; moreover it appeared that training for directly-relevant employment was the aim of the course. In other words, the universities feel sufficiently confident in the worth of their device to offer it as a passageway to not just graduate status but employability. The students have been enrolled (in both ANT and university senses), satisfied that they will be able to gain both skills and sufficient certification to start work.

An accusation of interest may be levelled at the universities (it is trivial to suggest that they have financial and other biases towards a graduate profession), however they do not have the monopoly on it. A practitioner network led by those without vocational degrees would disqualify themselves by agreeing to a graduate test! This is the effect in the network of the flux noted above: there might be network resistance from the “vanguarders” to such a minimum level of qualification which does not support their personal claim to competence. Any effect which arises is likely to be unstable, since the “practitioner” black-boxed actor is again unpacked, with the graduate internal stratum replacing their predecessors in senior posts. Given the expansion in the industry driven by government action to introduce academic quality standards, the network surrounding the symbols of qualification can be expected to be re-made on different lines as the occupation’s route to practice alters.

Courses available are run mainly by specialist security groups within university computer science departments, with a relatively strong emphasis on technical aspects compared to statute, auditing, culture, standards compliance or similar concerns. This suggests that Information Security has not seen within academia sufficient distinction or separation from security aspects of computing science to cause it to break away completely, although the groups may of course operate with sufficient independence for their own purposes. Whilst not at all precluding the teaching of non-technical matters (this was indeed observed as a minor component), course roots can be seen as based in technical concerns.

“[I]t's my mission to get computer science students and pour in security so it becomes a natural part of their research, their development, whatever they're actually doing.”
[EDU24E-CL05]

Similarly the government interviewee (himself an engineer by training) placed significant emphasis on security being mostly an engineering challenge for computing. Given that emphasis and that of the universities, it is therefore possible to speculate that there is some small disconnect or lag in the network, relative to the hypothetical ideal model for profession-building. The species of “security professional” conceptualised by the academic and governmental input here differs in substance from the less technically-dominant model exhibited by the practitioners and recent theory. This preparation is also at odds with the split of technician–specialist and manager–generalist needed to buffer the enforcement of policy away from the negotiation with senior management for its content. Where is the security officer trained if they are substantively different to the forensics and analyst specialities rather than simply promoted from them?

This disconnect may be explained from the academic side by history, but also perhaps by perception of the threat. Government is aware of significantly enhanced risk to itself (directly

and through loss of business tax revenue) from persistent sophisticated organised crime and state actor attack, against whom prodigious technical skill and analytic capability is required. It is therefore driving security partially as a response to that threat; even the “cyber” label of the CESG/NCSC qualifications standards carries overtones of Internet-based technical vectors. It has the power and intent to be a force for development of security but is not directly motivated to develop the profession beyond generating capability and capacity nationally. Pragmatically it needs security simply to have sufficient status not to deter STEM-oriented candidates from entering more established pathways and is not interested in delivering professional power and privilege, for example, or pay unless this was a factor in poor recruitment.

In an Abbotonian sense, there was evidence of this being an “opening up” of the knowledge base. The entry-level grade of the profession for which students appear to be being trained differs in emphasis from the one being practised in the field, however the education system is strongly motivated to train to the needs of employers since without marketability of graduates it cannot easily enrol students as an OPP to employment. The vanguard of generalist security managers, preside over growing security departments, now require analysts with greater specialisation both than they possess and needed themselves— note the number of technical roles in the proposed frameworks. Whatever tomorrow’s senior professionals will look like, therefore, the network will need to accommodate yet more change to the “practitioner” actor, and networks built upon its interests will again shift.

In terms of future developments, the question for the industry then is not whether to coalesce around the set roles created by the skills frameworks (potentially adding more) but whether first they represent specialties of the *same profession*, which appears to be in some doubt from this data. In the same way that medicine, law and other professions organise common teaching followed by specialisation, should forensics techniques and Information Security Management Systems be taught to all entrants? Should firewall specialists and policy creators begin as professional stem cells? It is not necessarily required that they use all the skills offered (there are elements to all professional training schemes which ultimately are not used) however the device used to interest an employer makes use of gravitas arising from that wide and deep education.

Variations in syllabus will occur unless controlled centrally. In the absence of a General Council-equivalent, the government has introduced a degree validation scheme which, whilst voluntary, will surely cause action within the marketplace. As has been seen with credentials, HR departments welcome easy mechanisms of selection; it must follow that graduates of “kite-marked” courses will ensure their badge is prominent when competing for employment.

Similarly those seeking the best education and most prized badge will naturally value those which are able to offer the quality mark.

As government is reacting to external stimulus rather than simply being capricious, this suggests that it might be reasonable to bias the workforce output of academia towards that stimulus. It is interesting however that this action had effect first on master's degrees, which at least one university reported being more popular with mature students in mid-career, looking to validate and develop that career rather than serve as its foundation for entry. Bachelor's programmes have gained in popularity and will now too be kite-marked, however one academic positioned the master's degree as more useful once the candidate had amassed more experience. Not all actors seeking a degree device then have the same motivation and thus will seek OPPs to differing states depending on their status and needs, thus government intervention may well have different effects in each market.

The government is acting in a space where tradition would expect a degree of self-regulation by the profession once a professional governing body had established itself. None of the educators noted action by professional bodies in the development of their courses however; it is possible that in this case change is so rapid in the industry that normal mechanisms cannot react requiring catalysis by those already in positions of power.

It is useful to maintain a distinction between human-centred Information Security which is part of the knowledge base, and "soft" inter-personal skills which are generally-applicable social and political tools in the workplace. As one interviewee mentioned, few people leave university as fully formed business professionals; much is learned by trial and error in early career. The literature however places emphasis on the substantial and theoretical business process- and culture-centred contexts to security practice, which *can* be lectured and examined (but may be harder than pure theory to appreciate outside a business context). As mentioned, previous entrants had received some exposure here having passed into the practice from outside, but this will need to be learned by direct-entry vocational graduates. Aspects such as culture, compliance, risk management and awareness appear to receive relatively little coverage in the institutions represented (although this was not necessarily to the personal satisfaction of the interviewee).

The existence of undergraduate programmes and the emphasis on preparation for work suggests that in principle a distinct, vocational occupation exists. The tension observed in one institution between offering training for industry qualifications and maintaining an academic-practice divide suggests that there is great potential for the industry to move to pre-registration graduate education followed by practice-based professional registration and qualification.

Conclusions relating to current status:

- Whilst the future Information Security workforce may be mainly graduate, due to the lack of clearly-delineated subordinate roles beneath a professional stratum, the identity of a distinct *graduate profession* with the characteristics of most accepted examples cannot develop. This is mainly a reflection of the relative immaturity of the profession. This leaves individuals to negotiate their place in the network without the ability to reference accepted status markers issued by a powerful professional body.
- The changes in industry practice and emphasis to require strong interpersonal skills, cultural understanding, empathy and a human-centred approach to corporate security are recognised in universities however the syllabus and teaching in the institutions represented still strongly reflects their computing science roots. Within the spectrum of courses offered there exist highly advanced and human-centric security programmes alongside more cynically-placed computer science programmes with minimal security content. As the professional bodies have yet to establish control over entry and hence develop the ability to dictate standards, government has acted in lieu of industry self-regulation in the market to introduce a voluntary quality mark, but with potentially high costs for universities to comply and the government choosing not to *impose* compliance, the effect is still limited.

Conclusions relating to future prospects:

- Acting in lieu of that strong professional body, government attempts to correct this lack of structure through the agency of role definitions are incomplete and not accepted as yet. Success may not simply be further structuring of a single-tier industry however, but considering tiered roles with a codified relationship to delineate the bounds of the superior profession. This is distinct from the hierarchical relationships within an organisation partially identified in the SFIA framework, as this does not necessarily reflect the hierarchy of status *between the professions* merely between workers. This requires the existing workplace networks to adjust to include new actors who import recognisable roles, probably using devices certifying their competence within that set role.
- Government's motivation to interfere in this area is pragmatic: to discharge obligations to solve an immediate skills shortage which is not being answered in the marketplace. Its action is not motivated to professionalise the industry for ideological reasons. Whilst its action will in some ways catalyse a process which might have happened naturally by

a professional body, this may be incomplete, for example in extending control over syllabus or entry to a professional body.

- The specialisation of junior technical roles in demand in the modern expanded and more mature workplace is higher than was the case for the generalist current managers during the infancy of the profession. The network black box entities of “practitioner” and “employer” must be unpacked, the former into “experienced” and “new” variants and the latter into manager and HR recruiter. The place of each in the network will evolve since practice is changing in nature as well as numerical strength during expansion, which will change the character and relationships of the central actor.

6.4 Professionalisation, Licensing and Regulation

The section above saw government intervening in the market for master's degrees (and only these, during data collection) due to concerns about the variable quality of syllabuses and the lack of a powerful intra-professional authority to approve courses. The sudden rise in demand for security workers created a pressure to add security content (at least superficially) to attract students, and hence gain funding. Whilst security will undoubtedly grow further in future, these actions are a reaction to market conditions and a lack of scrutiny, and not an *irreversible* translation of a particular actor's interests.

This can be observed in the network indirectly since some claimed security degrees do not survive scrutiny, creating a requirement to assess all. But there can be found no natural assessor where theory would expect to see one. The government reported being *by default* the focus of requests to test "security" degrees, to separate genuine leaders and the followers looking to capitalise on the market created without the requisite substance. This role is not yet being performed by an industry body, even though the execution of the policy *is* being performed outside government, thus it is apparently the *authority* which is lacked by the current professional bodies. Government did not ask for this role and does not display much enthusiasm for it.

Regulation in security is an area of flux. The data does not support there being a recognised single marker of competence in the field, thus in ANT terms no campaign by a candidate body has been successful in establishing itself as the OPP for entry to the profession either *de jure* or *de facto*. The literature for the Anglo-American professional model (such as that of Neal and Morgan, 2000) suggests that such a body would normally arise from those wishing to distinguish themselves, to certify members and unify the voice of the profession. There exist several candidate bodies, but with varying levels of commitment to seeking that OPP status for membership which would mark ultimate success. Certifications range from pure tests of knowledge (generally early-career level) to those which also require experience, ongoing training and commitment to ethical practice as a form of professional regulation. The latter resemble the route to chartered status exhibited by more established professions, which is important since these facets are thus known to be effective devices in similar networks and hence might cause similar effects in this developing network.

Some of the mechanisms for voluntary professional self-regulation are clearly therefore in place, but no network closure has been achieved. One failure point appears to be motivation, and not just that of one actor; as noted in the previous chapter, positive attitudes towards the desirability of professionalisation for its own sake were less visible in the data. Practitioners saw

value in *acting* professionally in the sense of competence and adherence to best practice, but were not especially drawn towards status in its own right. Mostly there was a feeling that this could be justified in principle at some future point however the profession is “not there yet”.

Neither is the network still in the stage of problematisation, staking out roles, however. Some parts show a clear acceptance of the proffered devices through to enrolment. Those looking to hire workers already appreciate a way quickly to establish competence as a minimum bar to sift CVs for example, the market penetration effects of the CISSP qualification being easily visible in this regard. Externally-validated testing discharges due-diligence obligations for management looking to offload risk for hiring decisions to credentialing bodies, which has achieved a degree of network stability. Yet the traditional motifs of seeking to exclude the incompetent and obtain control are not clearly present, contrary to expectations from the literature. None of the certification bodies made explicit references to controlling access to the occupation or to obtaining monopoly control. Whilst ANT can support unintentional translation of interests into action – which includes virtually all action by non-human actants – since there is usually considerable resistance to granting monopoly this is surely unlikely if it is not even being sought.

The educators were broadly very positive towards a more traditional route to professional formation, with graduate conceptual education being followed by postgraduate in-role professional certification. No sense of competition was observed between education and certification, with these seen as complementary, however there was considerable reluctance outside academia to embrace mandatory licensing, principally because it was not clear that there was an acceptable form of examination. When specific concerns about testing were put aside, generally the attitude towards some form of certified practice improved significantly. The onus is on the certification bodies to create an acceptable qualification regime.

Professional certifications however were the only available certificate mid-career for many of those currently in senior positions. They therefore occupy a place in the original network whereby they were the sole passage point. For any one qualification – in most cases based on a single examination – to bear the weight of attesting to similar status to those professions with multi-year graduate preparation and postgraduate supervised qualification is simply asking too much. It is enough to show intent, even basic competence, however it is probably impractical to establish status equivalent to law or pharmacy when the preparation and examination regimes for these are so much more rigorous, even if the certified individual could well have equal non-examined expertise and judgement amassed from pure experience.

Looking to the future, it is likely therefore that the occupation will have more success in

establishing itself when the professional body sets standards for experience and training but does not itself attempt to compete with university degrees as the benchmark for *learning*. This may also address the lack of gravitas mentioned by many interviewees. Whilst the IISP's model already appears compatible with this, the very widely-accepted CISSP qualification appears to sit uncomfortably between attesting to theoretical learning and certifying professional competence. For which service of which actor is it claiming OPP status? Conversely, the (ISC)² offers both basic and advanced qualifications which start to map to foundation and specialist grades of practice as well as recognising multiple sets of technical and non-technical roles alongside its flagship qualification; are these separate classes of actors? Or grades within a single class?

A substantial change in the network can therefore be predicted, so fundamental that the OPPs for proofs of learning and competence must surely shift. From the data it is possible to posit that the original audience for a security qualification had undergone non-security education and entered the workplace before or during the growth of security, probably in industry. Until a sufficiently large amount of distinct conceptual and abstract knowledge had been accumulated, it was necessary for academics to align very closely with the established field of computing science to develop enough material for a vocational degree, besides the necessary apparatus of teaching, research and examination. Similarly, during the initial stages of this growth the pioneers, who survived on practical knowledge gathered from any available source rather than built on specialist training, were creating a distinct profession with its own identity.

For the early workers therefore, many now in management and with many years' work supporting their authority, their principal claim to competence rests (or rested) on outright experience. Their negotiated position in each network was sold more on a personal basis according to their reputation and perceived skill rather than by a device during *interessement*. Their judgement comes from viewing both events and budgetary contests at first hand, which can be informed by both conceptual and technical training alongside that career but not ultimately dependent upon it. The more open-minded amongst them will possess sufficient reflexive vision to recognise the benefit of more directed prior training, however moves to make graduate preparation essential are likely to result in questioning scepticism unless reservations are addressed. In this group there was reluctance to trust any single qualification to be the arbiter of competence.

Although not as a group *implacably* resistant to requiring certification, no single spokesman in has convinced this group that it is able to represent them. Many have however enthusiastically embraced mid-career certification as a *highly useful addition* to experience; it is seen as both a

useful source of training and of value in the workplace for proving a *minimum standard*. Whilst the use of a device to persuade *others* of competence whilst lobbying for a place in the network is not unusual, surely the presence of a certification in that network to provide evidence mainly to *oneself* of competence is relatively rare. Whilst others during *interessement* might take a certification device at face value, without a security professional having an accepted and understood level of competence and training it is perhaps difficult to know what standard of training it represents to the other actors.

Any mimetic alignment with established professions such as medicine or law is therefore likely to be rewarded. The validity of testing initially for taught skills at university and then again for competent practice by the profession has been recognised in many areas. As universities seek to provide a more rigorous and organised foundation of skills and knowledge, the certification providers (who are not well-equipped to provide in-depth education but perhaps better placed later to certify competent peer practice) become better candidates for the role of professional association and ultimately (as genuine OPP to professional status) that of regulator.

No tension is therefore seen between academic and professional certification, indeed the two by their similarity to existing professional structures and their complementary measuring points are somewhat symbiotic *provided* they clarify their respective roles. In other words, both can exist in the network but only if they state clearly to other actors the services for which they are the passage point, otherwise the associations will be vague and easily broken by unintentional competition and confusion. From the data, it seems that to be accepted as OPP the profession must “own” its governing body and not simply be subjugated by a market-derived need to obey it, to the point that its authority is unquestioned and hence its certifications become automatically accepted as valid. At this point effective control of the syllabus will be with whomever the profession chooses to speak for them and the position of the professional body will be complete and the network stable.

To create an identity and a reputation takes time. When asked whether professional status was achieved, or when discussing why the status of the profession is less advanced than other comparable candidates, the overwhelming factor given was maturity. Information Security is still a new area of practice, in the process of defining itself and establishing its own identity, culture and place in the organisational hierarchy. This is held in *interessement* by constant change: needing to return to staking out positions and lobbying other actors. Ordinarily as waves of vocationally-recruited graduates have replaced the pioneers in the network, the whole network would gradually move through enrolment to form durable and repeatable links, being re-made with each iteration but not substantially changing. Perhaps unfortunately for the

smoothness of this process however, the movements of state actors and organised crime have meanwhile made this area of employment the battlefield for a proxy war between superpowers and supercriminals.

As with many conflicts, a rapid expansion in reasonably well-trained infantry is required, hence the creation of a technically-focussed STEM graduate cadre of security analysts by the UK Government, fearing attacks on not just UK companies but itself and the national infrastructure. Its usual course of action (to leave professions alone unless and until persuaded regulation is desirable) has been perforce altered by its own position as customer for that infantry. As the relevant network around cyber-training has not been established, it has stepped in to create it.

This creates several issues for the professionalisation project however. Firstly it hugely skews the network towards the flighty requirements of that powerful government actor, which can impose and cajole in the absence of a professional body but it cannot force trust and acceptance in the existing profession. There was significant resistance seen to the concept of government administering the profession itself, mainly from a suspicion that government is not competent to do so. Government is therefore in a difficult situation: to catalyse development it may have to interfere using its well-respected security brands, however if it were to appear to be not simply supporting but imposing a system not yet accepted by the profession, it may in fact damage the credibility of the institution it seeks to empower.

Secondly, government reports not *wishing* to administer the profession and neither does it wish to interfere in the market any more than is necessary to complete its tasks. Thus again it is interested in ensuring that security has sufficient recruits and they are not dissuaded by the perception of security as a less prestigious option, trained by competent people and recognisable, however again this is output-driven rather than ideology-driven.

The creation of a profession from an occupation which is widely practised without formal central organisation is to move a micro process to a macro process. An occupation comprises multiple individual examples within organisations of individuals or functions claiming to be the OPP, in this case for the fruits of proper secure practice. To form a *profession* requires action on a macro scale, where government accepts a body speaking for an industry as the OPP to the general national benefits of well-run Information Security.

That body must therefore enrol its individual members because without a police force and the mechanisms of state it must win positive consent for representation. Whilst overt government action to assist the sell may temporarily assist the formation of some species of association, it skews *interessement* by changing the interest and identity of the actor seeking the advancement

of the profession. The GCHQ badge for degrees is a device of *interessement*, but not directly on its own behalf. An irreversible network is more likely to be formed when a professional body legitimately achieves the translation by itself.

Government's instinct was to regulate *externally to the profession* (by the industry's regulator). This would be rather unusual, although the classic case of regulation entirely within the profession is now also not the norm. Medicine for example is regulated through the General Medical Council (with lay if knowledgeable council members) and physicians' employment interests represented separately through the British Medical Association. Similarly the regulatory and representative functions of pharmacy and law have been split recently. A recent trend for state-sanctioned delegation for regulation therefore is to a regulatory body ruling on fitness to practise and syllabus. Whilst even the pure-regulator approach could organise the training and certification profession, it is clear that at the moment the government has not been enrolled into a network by such a regulator. It is similarly not clear that any of the candidates is exerting itself with any passion in any case, nor that the profession is particularly exercised by the concept.

Conclusions relating to current status:

- No competition was seen between academic and professional qualifications. The latter were however seen only to establish a baseline minimum of expertise rather than establishing a state of "qualified" comparable to chartered professions. Security is not always regarded as an area which requires advanced learning to practise, which in turn challenges the overall status of the profession.
- There is little appetite from the existing professionals (many of whom could be thereby disenfranchised) to exclude people from the profession based on certification, with exclusive models of profession also rejected. Whilst there was strong support for licensing *if* a suitable test could be found, no such test was accepted as yet. There was rejection of there being a compelling need to exclude the incompetent. Whilst there may be a social disincentive to admit to favouring exclusion and elitism, without a desire to achieve some degree of monopoly or self-control the traditional network is more difficult to form irreversibly.
- Government has introduced its own certification standard to catalyse the industry but does not wish to appoint any existing body as a regulator at this time. The data suggests that government is correct to be wary of intervening further but for other reasons. Government reticence stems partially from liberal non-interference in a free market and

partially to avoid the necessity of supervising the resulting professional body, whereas resistance to government-imposed certification from within the profession was due mainly to lack of trust in government's ability to do so competently.

- Government has acted because it requires the creation of clear and effective pathways towards employment in a network where there is no ambitious candidate regulator representing the will of a profession aiming to establish a form of control over entry, training and behaviour.

Conclusions relating to future prospects:

- Professional certifications give confidence to existing professionals who trained before academic qualifications were available and which therefore serve as a single certificate to attest to learning and competence. Greater graduate entry may force some certifications which test *knowledge* to position their products instead as post-graduate markers of professional experience, skill and competence, and hence raise standards beyond “basic minimum” level. This movement may in turn assist in the rationalisation of certification schemes as universities move to be the sole OPP to recognition of learning.
- Rationalisation is needed in the market for certifications alongside the codification and stratification of roles such that the occupation has well-defined borders with a single qualification per role. At present the binary status of “qualified” or “not-qualified” is diluted by a high number of certificates of variable quality.

6.5 Summary

“The observer does not fix the identity of the implicated actors if this identity is still being negotiated.”

[Callon, 1986]

Arguably, to streamline education, qualification and organisation of a profession it is necessary to provide and examine a general level of knowledge which can then be built upon to provide the foundation to a finite number of specialities. Beyond these practical concerns, common socialisation and training helps to solidify the identity and image of the professional *qua* doctor, lawyer and so on, applying a broad background knowledge to the client’s situation rather than merely possessing those facts needed for their particular task.

It is therefore to be expected that the role of Information Security professional, in order to progress from the status of self-certified keen amateur in a nascent offshoot of computing to a “professional” role with all that entails, should need to adapt. Professions exist to control practice in an area of knowledge according to society’s overall division of labour. A common body of knowledge must therefore be established and demarcated, a separate identity forged, internal roles defined, a hierarchy and web of peer relationships agreed, training regimes for each role created, and standards set and tested. A discrete area of knowledge must be controlled by those who claim that expertise, thus the profession must associate to codify that knowledge, agree and publish best practice for its associated techniques, establish of a bar for qualification according to grade, and create and (nominally) enforce a code of ethics. A professional body homogenises the variable knowledge and practices of individual constituents into standards. It defines what a professional does and what they know, and decides who is and is not a competent professional, firstly by voluntary membership and eventually by state-sanctioned monopoly.

In principle many of these traditional network elements of association have met or been brought together in the case of Information Security, however there are areas of failure to achieve mobilisation and translation on many fronts. Perhaps since *failure* implies attempt and defeat, which is not the case here, a better term would be *as yet incomplete*. The areas at issue have been explored over the preceding sections: diffusely demarcated base of knowledge along the borders with the parent professions such as audit and computing, lack of confidence and aspiration to professional status, lack of clarity of roles between internal specialities, very rapid change in practice, changes in motivation and expectation between generations of workers and incomplete establishment of a graduate, highly-educated identity.

Furthermore it was seen that although much of the apparatus of professionalism has been established, the role of professional body and its credentials are still very weak. Note the recent

direct government action rather than autonomous action by the profession, severe over-population of the credential market leading to confusion about a substantial and qualified status, lack of status and “gravitas” parity with comparable professions and – inevitably given the above – failure to enrol government into granting monopoly control.

Underlying all these – including and perhaps *especially* the lack of aspiration to professional status – is *time*. The lack of definition visible in the accounts of the interviewees and other data is no coincidence, since this network is still forming. Fundamental to ANT (see Latour, 2005; Callon 1986) is that the identities and roles played by actors are not hard and ready-made Social Things which can be imported whole into interaction, but rather they are formed and shaped *by and during* that interaction. Some interfaces and negotiations may be simpler than others, however it will be by repeatedly forging and testing links, negotiating positions and defending ground gained until the network is stable and irreversible that a true profession will be formed.

Few of the remaining issues are likely to be fundamentally fatal. The relationship between multi-tiered specialist practitioners in large multinational and governmental departments and those in smaller SME departments is not incomparable to research–industrial and community pharmacy for example. Several certification providers offer multiple grades of general and specialist qualification, therefore the main issue appears to be rationalising to a common scheme or set of standards. Whilst IT forensics and fostering an awareness culture seem distant cousins, modern medicine claims psychiatry and pathology within the same profession with common basic training despite wide variations in practice, and due to a powerful regulator can force entrants to choose a speciality rather than practise in an ungraduated spectrum. All such issues of identity and qualification have been faced and solved through negotiation and political interaction in many other professions. Even the currently unpersuaded government may alter its stance should a powerful, well-organised and competent professional governing body offer itself for consideration.

The current status therefore is of an incomplete network still in the process of *interessement* and the early stages of enrolment. A remaining question, which this study hands over to later writers to answer, is simply that of resolve. At present there is some progress but considerable caution towards seeking professional status due to the unresolved issues above. When these are addressed, the way is open for the coming generation to achieve full professional status. The key question will be: will they want it?

Chapter 7: Conclusions

In the following chapter the conclusions of the work are summarised and juxtaposed with the research questions identified in the literature review, the contribution to knowledge summarised, implications for theory and practice noted and limitations discussed.

7.1 Answers to the Research Questions

7.1.1 Question 1: “What are the Origins of the Modern Information Security Profession?”

Focus Question: “When and why did Information Security roles emerge and separate from Information Technology to form a new profession?”

Section 6.1 showed that the participants included people who had observed the emergence of the Information Security profession within their own careers. Some indeed had identified the need for (and sometimes created) their own security function around them, recalling contemporary Information Security as effectively non-existent. No single cause for the advancement of security as a specialist concern was identified from the data; rather, interviewees noted a range of events and trends which for them were significant. A key factor noted was the expansion of the Internet in the early 1990s since from this the abuse of its associated applications became possible, such as mail-borne viruses and attacks on remote infrastructure. As a response, data protection legislation, security standards of increasing complexity, the development of online commerce and similar issues emerged. With *each* such development the pressure to secure the computing environment increased whilst the cost of effectively acting maliciously decreased.

There was therefore a range of threat vectors, of which a subset were felt to have particular effect in a given interviewee’s particular context and others were seen to be more general in their action. Most significant is to note that the *technological change* which made malicious action possible and the changing motivation of *human actors* who perpetrated it are inextricably linked. It was the *combination and interaction* of these which brought forward the conditions to which security expansion was a response, which is revealed more clearly by an ANT account.

The new profession faced challenges, since its effect was unintentionally to hinder the pursuit of computing performance which, since contemporary hardware capability was orders of magnitude below today’s standards, was a significant issue. Additionally, to win acceptance of let alone impose policy required senior management buy-in. Effective security managers as now required adroit political and social skills in addition to an understanding of technical matters. By

combining inputs from the literature and this empirical observation it is concluded that it was this new class of worker – grounded in the technical context but gradually embracing the social, legal and behavioural aspects – which formed the basis of the new profession in an Abbotonian manner.

Following the emergence of malicious activity, associations of workers with like interests were formed, which influenced recruitment patterns for the few early roles which were gained primarily by personal recommendation. Expansion of the profession caused a test of security competence to be needed as existing methods were not scalable. This change of mode from intensive but subjective vetting to objective but impersonal testing changed entry routes and hence the nature of the profession. It is this *change* which has the potential for most significant development.

Qualification allowed the profession to claim status through competence certification in a specialist field issued by an authoritative body. Possibly just as important however is the inward confidence that was gained for an otherwise unqualified occupation, now having an objective platform from which to pass judgement upon others during audit and policy enforcement. Hallmarks of profession are no guarantee of acceptance however, therefore in the next section the current status of the profession is examined.

7.1.2 Question 2: “What is the Current Status of the Information Security Profession?”

Focus Question: “To what extent does a discrete area of practice exist with which the practitioners associate and what is its status?”

There is clear evidence for a separate area of practice backed by a claim to an independent body of knowledge and theory, which can be taught to postgraduate level and certified by occupational qualifications. Information Security is demonstrably a candidate profession in that sense. There are however a number of challenges to the professional status of the occupation, mostly due to the short period of time which has elapsed since its separation from its parent areas of practice.

In section 6.2 it was argued that the area of knowledge claimed is too broad to be mastered without specialisation; a key criticism made of the most popular certification is that it is too broad and too shallow to establish expertise. Sophisticated frameworks exist to support the codification and organisation of the profession however there remain no *well-accepted and understood* named roles for Information Security workers in the industry. This effectively prevents the formation of networks of peers, clients and staff based on the claims of professional

qualification. This in turn compromises the status of the profession with respect to more established peers. Instead the individual's own personal attributes and skills determine their acceptance into locally-negotiated hierarchies and role networks, whereas those working in more established occupations can derive status more easily from legitimation through acceptance by their own profession.

Further ambiguity surrounds the internal structure of the profession, with regards to the hierarchy between and nature of specialities of professional and any support workers. As above, where relationships are negotiated in the work context both around and within the area of knowledge claimed, security specialists cannot easily refer to an existing accepted structure, leaving the individual to position themselves based on their own identity rather than their professional identity.

The social–technical axis was identified as the most significant source of this ambiguity, with tension observed between those who execute security policies and investigate non-compliance, and those who interface with senior management (to obtain resources and assent to create policies) and drive security awareness and culture. The distinction observed exceeded normal hierarchical control between management and staff and provides an empirical basis to propose specialities with discrete skill sets. Furthermore, the technical group was not seen to aspire to progress to the management group nor saw it as superior. A symbiotic relationship is formed comprising the security manager as resource-provider to the technicians and insulation from management, in return for nominal superiority in *organisational* hierarchy manager to specialist, but not a *hierarchy of specialities* comparable to physician and nurse.

Whilst few practitioners would advance Information Security as comparable to those professions which are entrusted with the vital interests of clients, there was felt to be sufficient potential in all relevant characteristics to advance to reasonable recognition in future. In section 6.4 it was noted that current professionals, who could be thereby disenfranchised, showed little desire to exclude incompetent people from the profession based on certification, rejecting such exclusive models of profession. Whilst there was support for licensing if a suitable test could be found, no such test was accepted as yet.

Taken together with the discussion of education and certification in section 6.3, this strongly suggests that there is no current body in a position to command the respect of the profession and hence drive the professionalisation process further, and certainly the language of the bodies interviewed did not support the highly monopolistic orientation suggested by the sociology of professionalisation. Empirical corroboration is given here of suggestions in the literature that rationalisation is needed in the market for certifications alongside the stratification of roles

noted above. At present there is an insufficiently clear binary status of “qualified” or “not-qualified” due to the presence of multiple certificates of variable quality.

The profession then must mature in both structure and training to gain full acceptance from their peers. Influence at management level is still reliant on occasional crises and outside these events resources must be continually re-won, showing that other, more powerful actors are still out-competing the profession for the attention of management.

7.1.3 Question 3: “What Are the Prospects of Further Professionalisation?”

Focus Question: “Are there ongoing projects to professionalise the industry, what are their aims and are these being achieved?”

One must consider here the question of the polysemy associated with Ritzer (1973) and later writers, in that efforts to professionalise might be validly seen as the pursuit of *status*, the *trappings* of a profession (regulation, certification and so on) or simply striving for high quality, competent and conscientious service regardless of trade. Since the latter would be difficult to achieve in a concerted manner outside the framework of an organising body, it is the former senses of the word which are most relevant.

Firstly, in as far as people could be expected to admit to such things, in section 6.4 the pursuit of professional status as an end in itself was not seen particularly to motivate current practitioners. For even senior and self-confident professionals who were otherwise relaxed and comfortable during interview, this topic elicited hesitant and exploratory responses, suggesting that it was not something which had previously engaged their interest. If this particular sample’s attitude was considered on that specific point then the actions of government – to reposition the industry such that it does not lose entrants to more respected competition – might be misguided.

This said, the sample was comprised of people already recruited into the profession, mostly socialised, educated and trained outside the profession, or indeed before the existence of the profession. Whilst the network has formed around *their* interests as they have established themselves, it is likely that they will gradually be replaced by successors who positively chose a career with an established identity against competing opportunities, thus status could well be a relevant factor. There was evidence in section 6.2 however that this identity was still not well-known even within enterprises already employing a security team, therefore this factor would be of limited relevance to school leavers had they not already been otherwise attracted by personal interest.

In sections 6.2 and 6.3 this lack of identity, organisation and gravitas was seen severely to hamper the progress of the profession. It is doubtless that government, which showed no desire to interfere unnecessarily in the market, has nonetheless been *forced* to catalyse and develop the industry through its interventions in the areas of academic and professional qualifications, and the establishment of a more clearly delineated and defined discrete set of roles as discussed above. Government, unusually for Anglo–American professionalisation, was made to encourage a currently immature profession to develop more quickly, due to the rise in malicious activity and thus national demand for skilled workers.

But government motivation to interfere in this area is mainly pragmatism: it must respond to a demand which cannot be sated through the normal course of events. It has no ideological commitment to professionalisation in its own right. Whilst it may in some aspects simply *catalyse* the process, this may remain incomplete for aspects not seen as useful for its purposes, for example extending control over syllabuses, and it strongly rejected requiring membership of a governing body for entry to the profession. Its actions have replaced those which would have normally been expected from a professional body emerging by popular subscription from amongst the profession itself, however no such body has convinced government of the necessity to regulate the profession; establishing a full articulated profession is clearly some way off at this point.

Resistance to government intervention was not the monopoly of government itself. Whereas government reticence to regulate came from both non-interference in a liberal free market and not wishing to supervise the resulting regulator, government oversight was rejected by some of the practitioners themselves citing its record in doing so competently elsewhere. It appears therefore that further professionalisation is predicated on the establishment of a strong professional body who can offer a test acceptable to the industry and then advance its cause. When questioned assuming the existence of an *acceptable* test, resistance to mandatory certification was lowered. The resistance was seen to be mainly that of trust in the testing authority rather than implacable ideology.

In section 6.4 the field of certifications was seen to be a further obstacle to future progress. For existing professionals, who generally entered the profession before vocational academic qualifications were available, these acted to increase confidence and to attest to learning and competence. Nonetheless, the plurality of schemes available suggests variable standards and thus damages the perception of all. These must clearly be rationalised (despite opinions to the contrary from both government and – counterintuitively – the certification bodies), but they must also adapt to the emergence of academic qualifications. The current “home study and

single exam” schemes, whilst fit for their original purpose of proving a basic minimum, were seen as far too insubstantial to grant genuine *professional* status on such a very limited engagement. In future, with greater graduate entry and socialisation, it is likely that the industry will force certification paths towards the more common undergraduate teaching of *knowledge* and postgraduate certification of *professional competence*, and thus raise standards. This is closer to the peer-reviewed IISP model than the current examined certifications.

Looking to that undergraduate pipeline, the change in formation routes, whilst encouraging depth and breadth of curriculum, brings challenges. Changes in industry security practice, the recognition of human aspects of security and business-centred emphasis require strong interpersonal skills, cultural understanding, empathy and a human-centred approach to corporate security. There was evidence that this was recognised in universities however whether this was being incorporated into syllabuses and teaching was less clear, with courses strongly reflecting their roots in computing. As no professional body has yet to establish control over entry or ability to dictate the curriculum, something which the literature demands for professionalisation, government has again acted in lieu of industry-generated initiatives. The existence of a government-backed quality mark was seen to have had some effects, however given the high compliance cost and the voluntary adoption model, the effect is still limited.

In summary, many of the necessary foundations to greater professionalisation are in place however the industry has yet to fully embrace and demand certification rationalisation and regulation, and without this any attempt to lobby government (which is already resistant to introducing such regulation) is unlikely to be sufficiently well-coordinated to be effective.

7.2 Theoretical Considerations

7.2.1 The Contribution of Actor–Network Theory

This study highlights the value of ANT for enriching a professionalisation account. Beyond the convenient taxonomy for the constituent stages of social action provided by Callon (1986), it provides a model for the negotiation of reproducible and settled arrangements between actants.

Harmony is evident between focal actants as “OPP” and the centrality of monopoly to theories of professionalisation as market closure (see Fig.7 in section 3.10). An actant seeking to enrol and represent others and protect their interests—as part of advancing its own—is literally true for the traditional professional body as gatekeeper to its members’ services. An array of devices of *interessement* is visible in Chapter 5 in their attempt to recruit practitioners, employers and the state as allies. By adopting the viewpoint of each focal actor as OPP in turn, it was possible to

show not simply how the network was built, but also how it adjusted to *change* by renegotiating the interrelations between its constituent objects during the introduction of a new actant. This contextualises Neal's (2008) theoretical maturity and separation model of enterprise security, by showing how the new function becomes OPP to desirable new states for pre-existing actants.

Also useful is ANT's micro-social ontology, described in section 3.4. ANT rejects macro-social forces, requiring accounts of action to identify assemblages of a plurality of elements, similar to Latour's *gun-man* example. It prevents the ascription of security's emergence and separation to "power" or "class"; it is instead shown as the product of a momentary convergence of *both human and non-human artefacts*. The development of the web, browser and DSL technology driving online human consumerism and social media usage, and consequently social engineering, malware, data protection legislation, breaches, executive liability and security standards—amongst other factors—produced conditions wherein a security specialist could develop. Moreover, both policy creation and policy enforcement workers find opportunities to be employed and to negotiate their roles and relationship in a changing technical and statutory context. The importance of ANT's generalised symmetry, which treats these disparate materials as fully equal in potential, is thereby demonstrated.

ANT is similarly helpful for describing the failure of a network to achieve a stable and repeatable end-state. The inability of spokesmen to deliver what they claim to represent (or "mobilise" others) can be seen. Cynically designed degrees have failed to represent proper training, thus the network developed additional tests and standards to reject them. Certifications designed to create a basic baseline have been positioned as attesting to education similar to comparable professions, but failed to establish comparable substance to those professions and hence fail to attract the same power and status. The ANT concept of the "black box" can likewise be used to represent the established professional model, where the term is so ingrained into common conceptions of occupational status and gravitas that it is referenced without examination by government in its strategy, and to the action of standards whose contents are in reality less relevant than their market acceptance.

7.2.2 Professionalisation Theory

Within the professionalisation arena, the work of Abbott (1988) was the foundation for much of the analysis, and proved particularly well suited to an ANT account. Informed by this work, for example, the emergence of the IISP alongside the BCS was seen as potential evidence of fracture and dissatisfaction with the status quo by specialists within existing professions, following the establishment of new areas of knowledge through socio-technical development. The failure of the BCS to be a "spokesman" for the emerging discipline is particularly

reminiscent of the narrative in Callon's (1986) seminal paper. Similarly, the dynamic nature of Abbotonian formation and the continual renewal of what appear to be fixed boundaries, especially before state monopoly (compare ANT's *irreversible translation*) is achieved, is aligned with ANT's major themes.

Perhaps the most notable contribution of Abbott to the key question of security roles, since the prior work here has very limited theoretical foundation, is during the discussion of role networks (section 6.2). This finds resonance in the unresolved tensions reported here concerning what constitutes the outer edges of the entire profession, and the arrangement and hierarchy of any constituent specialisations and/or para-professions— aspects overlooked in previous studies. Abbott and Larson showed that control over a discrete area of knowledge—its education, socialisation and practice—is central to a professionalisation project, underpinning the conclusions above that resolution of role identities, then rationalisation to a unique and highly abstract certification path for each is a prerequisite for further professionalisation.

Beyond Abbot, in section 2.3.4 substantial criticism by writers such as Freidson and Larson was reported regarding the unwelcome effects of monopolistic ambition and market closure. Strikingly, contrasting positions from this were observed in the data. Practitioners were resistant to modes of licensing which would exclude existing currently unqualified peers (contrary to even the moderate theoretical orthodoxy), and even the professional bodies rejected this despite a clear contrary financial motive.

Similarly, assertions by Freidson that professions inevitably act to constrain their clients were refuted by the highly business-oriented data reported in section 5.6. The still extant calls in the literature for a more socially-informed approach to security may therefore have more resonance in academia than enterprise. Conversely, writers who stressed the contribution to the public good made by professionals through their altruism (section 2.3.2) would doubtless be surprised how sparsely this argument was advanced here.

Building on theoretical discussions of definition, absolute precision appears here not to be useful, since professional status has become black-boxed and thus referenced without detailed examination. When attempts are made to use that understanding to form policy however, as was done for example by UK and US governments, an *insufficiently developed* understanding of professional models and development can lead to errors of assumption and over-simplification. The historical literature examined in section 2.3, for example, suggests that Anglo-American professions evolve gradually by fracture, competition and consolidation prior to seeking state recognition. Government catalysis to solve its immediate recruitment issue may be precipitate and even counter-productive in the long term.

7.2.3 Socio-Philosophical Considerations

From a methodological point of view, whilst the appeal of generalisation is appealing to some as noted below, this work strongly supports the use of interpretative, qualitative approaches in professionalisation studies. This approach may avoid the false appearance of unity of mind which can lead from the statistical treatment of survey data within a more traditionally positivist epistemology, particularly in areas where the underlying theory is not well developed. Many of the earlier examples of such work in compliance programmes were somewhat unsatisfying in developing truly useful directions for developing user education programmes, whereas a move to include more interpretative work could be helpful in exposing why human actors do not behave as intended.

7.3 Implications for Practice

To summarise the implications for practice from the main text above, these relate to the areas of *role* and *licensing*. As noted, the impact of the various frameworks has not yet been sufficient to create well-accepted roles within a hierarchical functional or power relationship, which was seen to prevent the occupation presenting an image of established professional status. Discrete specialities will therefore be needed prior to further professionalisation, ideally with a single certification path per identity to establish a condition of “qualified”. Certifications at present are not perceived to have sufficient depth for the holder to rank amongst peer professions.

From theory and observation here to attain that status is likely to require the occupation to become a graduate profession, thus existing certifications which currently attest to education will need to cede this to the universities in return for the status which derives from granting recognition to degree courses, wresting this from government. In turn the professional bodies will ultimately need to gain government sanction to license, to restore a role for a rationalised subset of their certification schemes. Government, which aims not to interfere in the market, may inadvertently so do by its actions in the certification and education sphere intended to catalyse the industry, which may be misguided if they do not convince the industry that it is not *imposing* a solution, whereas supporting a practitioner-respected body may be more effective.

7.4 Contribution to Knowledge

Whilst Information Security itself is the subject of considerable study, the professional status of the practitioner has received relatively little coverage therefore this study is an early work in what it is hoped will be an expanding field. Taken with the published interim findings, this study is the first academic work to consider the professional status and licensing of Information Security in the UK in depth, and the first academic work to analyse that status informed by a substantial coverage of the major sociology of the professions. It is the first work to cover this status using an interpretative approach and adds to the demonstration of Actor–Network Theory as a valuable analytical tool in the study of professionalisation. It provides empirical contrast to and analysis of the published policy direction of the UK Government and is the first academic work to include interview data with the department responsible for the development of that policy on this topic.

7.5 Limitations

The following principal limitations are acknowledged:

- **Size:** This is a small-scale study, particularly with respect to the non-practitioner categories of interview. As noted in the theoretical review, this is an interpretative and qualitative study which does not seek to establish highly generalisable statements concerning the behaviour of the populations. It is a descriptive ANT account which represents a commentary on the movements of actors seen in the data gathered. The size of the study was limited by the time available, the travel resources and the single-student capacity for interview administration, execution, transcription and analysis. In particular a greater response rate from academics might have enabled greater comparison between practitioner and academic positions on areas of mutual interest.
- **Time:** Conversely, the data collection took place over a multi-year period in a relatively new and fast-moving area, therefore the interviewees at different stages of the research may have been speaking in different contexts with respect to then-current issues, government action and development. Given the level of activity of GCHQ and the Skills Frameworks for the Information Age for example, it is very likely that the position of the UK Government will be changing regularly and may have been developed since that data was collected.
- **Cultural Issues:** The model of professionalism, the government's intervention and the attitudes to professional development all apply mainly to the UK.

- **Participant Recruitment:** The participants were all volunteers, and in the main were recruited by response to an impersonal request for assistance. As this requires considerable altruism (particularly given the amount of time required from very senior people in their respective organisations) this may have affected the representativeness of their attitudes to professionalism relative to the general population.

7.6 Recommendations for Further Work

Although this is a relatively new field and much can be usefully done to explore it further, the following areas may be profitable lines of research in the immediate future:

- There is likely to be an effect from the changing nature of practitioner recruitment from mid-career generalist to graduate- or postgraduate-entry specialist, thus the attitude of the students being socialised at university and the school-leavers making their degree selection is also highly relevant. Although an interview protocol was created and ethical procedures completed to include students into the study, it was not finally practical for both time and access-to-data reasons to do so. To explore this area of the topic would make an extremely helpful complementary study. Similarly, to expand the observed network further those who employ security staff may be able to offer a different perspective concerning certificates and other symbols of professional status, as would to include those working in the security products industry whose voices were not heard here.
- The context for practice in this industry is *extremely* fast-paced. As was noted above, there is a possibility that due to the novel influx of graduates and the changing global security situation affected the data collected even within the time of this study. It would therefore be useful repeatedly to explore the topic with workers in the industry and particularly within the (very active) UK Government to determine the direction of this critical area of movement, both longitudinally within a speciality (the nature of change) and across the profession's entire jurisdiction (the breadth of body of knowledge).
- As was helpfully identified by an anonymous reviewer of the paper linked to this project, it might be useful to compare the attitudes of the classes of workers covered in this study with those of other countries. As the type of professionalisation assumed is the "Anglo-American" model, the data might be usefully combined with that from the United States in order to compare results in different regulatory cultures to determine whether different governments' actions and different cultures produced similar findings. Similarly the experiences of those workers in a French, German or similar non-

Anglophone culture could be extremely instructive.

- Having exposed some concepts from this small, qualitative data set, those who prefer to take a positivist and realist approach might wish to derive hypotheses to extend generalisability, in order to determine to what extent unity can be claimed for one or more of the stakeholder groups overall.

References

- Abbott, A. (1988) *"The System of Professions: An Essay on the Division of Expert Labour"*, Chicago: Chicago University Press.
- Adams, A. and Sasse, A. (1999) *"Users Are Not The Enemy"*, Communications of the ACM, Vol. 42, No. 12, pp.40–46.
- Adams, T. (2015) *"Sociology of Professions: International Divergences and Research Directions"*, Work, Employment and Society, Vol. 29, No.1, pp.154–165.
- Adnan, M., Just, M., Baillie, L. and Kayacik, H. (2015) *"Investigating the Work Practices of Network Security Professionals"*, Information and Computer Security, Vol. 23, No. 3, pp.347–367.
- Ahmad, A. and Maynard, S. (2014) *"Teaching Information Security Management: Reflections and Experiences"*, Information Management and Computer Security, Vol. 22, No. 5, pp.513–536.
- Al-Awadi, M. (2009) *"A Study of Employees' Attitudes Towards Security Policies in the UK and Oman"*, Unpublished Ph.D. Thesis, Glasgow University.
- Albrechtsen, E. (2007) *"A Qualitative Study of Users' Views On Information Security"*, Computers and Security, Vol. 26, pp.276–289.
- Albrechtsen, E. and Hovden, J. (2009) *"The Information Security Digital Divide Between Information Security Managers and Users"*, Computers and Security, Vol. 28, No. 6, pp.476–490.
- Albrechtsen, E. and Hovden, J. (2010) *"Improving Information Security Awareness and Behaviour Through Dialogue, Participation and Collective Reflection. An Intervention Study."*, Computers and Security, Vol. 29, pp.432–445.
- Alexander, P. (2008) *"Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers"*, Santa Barbara: Praeger Security International.
- Amsterdamska, O. (1990) *"Surely You Are Joking, Monsieur Latour!"*, Science, Technology and Human Values, Vol. 15, No. 4, pp.495–504.
- Anderson, J. (2003) *"Why We Need a New Definition of Information Security"*, Computers and Security, Vol. 22, No. 4, pp. 308–313.
- Anderson, R. and Moore, T. (2007) *"Information Security Economics – and Beyond"*, IN: Menezes, A. (Ed.) *"Advances in Cryptology - CRYPTO 2007 Lecture Notes in Computer Science"*, Berlin: Springer, pp.68–91.
- Andrews, M. (2016) *"Durham University: Last of the Ancient Universities and First of the New (1831–1871)"*, Unpublished D.Phil. thesis, Oxford University.
- Ashenden, D. (2008) *"Information Security Management: A Human Challenge?"*, Information Security Technical Report, Vol. 13, pp.195–201.
- Ashenden, D. and Sasse, A. (2013) *"CISOs and Organisational Culture: Their Own Worst Enemy?"*,

Computers and Security, Vol. 39, pp.396–405.

Atkinson, C. and Brooks, L. (2003) "*StructurANTion: A Theoretical Framework For Integrating Human and IS Research and Development*", AMCIS 2003 Proceedings, Paper 378, pp.2895–2902.

Ayoub, R. (2011) "*The 2011 (ISC)2 Global Information Security Workforce Study*" [online], Available at: <https://www.isc2.org/uploadedfiles/landing_pages/no_form/2011gisws.pdf> [Accessed: 10/10/2016].

Backhouse, J., Hsu, C., and Silva, L. (2006) "*Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard*", Management Information Systems Quarterly, Vol. 30, pp.413–438.

Barlow, J., Warkentin, M., Ormond, D. and Dennis, A. (2013) "*Don't Make Excuses! Discouraging Neutralization To Reduce IT Policy Violation*", Computers and Security, Vol. 39, pp.145–159.

Barton, K., Tejay, G., Lane, M. and Terrell, S. (2016) "*Information System Security Commitment: A Study of External Influences on Senior Management*", Computers and Security, Vol. 59, pp.9–25.

Baskerville, R. and Siponen, M. (2002) "*An Information Security Meta-Policy for Emergent Organizations*", Logistics Information Management, Vol. 15, No. 5, pp.337–346.

Baskerville, R. and Wood-Harper, T. (2002) "*A Critical Perspective on Action Research as a Method for Information Systems Research*", IN: Myers, M. and Avison, D. (Eds.) "*Qualitative Research in Information Systems: A Reader*", London: Sage, pp.169–190.

Becher, T. (1990) "*Professional Education in a Comparative Context*", IN: Torstendahl, R. and Burrage, M. (Eds.) "*The Formation of the Professions*", London: Sage, pp.11–23.

Bell, D. and LaPadula, L. (1973) "*Secure Computer Systems: Mathematical Foundations and Model. Technical Report M74-244*", MITRE Corporation.

Bennis, W. (1973) *The Times*, 24/9/1973, p.20.

Berg, B. (2004) "*Qualitative Research Methods for the Social Sciences*", 5th Edition, Boston: Pearson Education.

Bernard, R. (2000) "*Social Research Methods: Qualitative and Quantitative Approaches*", Thousand Oaks: Sage.

Besnard, D. and Arief, B. (2004) "*Computer Security Impaired by Legitimate Users*", Computers and Security, Vol. 23, pp.253–264.

Bird, P. (2009) "*Methodological Issues in a Study of Mobile Learning as a Disruptive Innovation: Actor Network Theory and Case Study Unit Analysis in a Qualitative Study of Three Mobile Learning Projects In UK Higher Education*", 16th EDAMBA Summer Academy, Soreze, France [online], Available at: <<http://www.edamba.eu/userfiles/file/Bird%20Peter.pdf>> [Accessed 07/04/2012].

Blakley, B., McDermott, E. and Geer, D. (2001) "*Information Security is Information Risk Management*", IN: "*Proceedings of the 2001 Workshop on New Security Paradigms (NSPW '01)*", Cloudcroft, New Mexico, 11th–13th September, 2001, New York: ACM, pp.97–104.

- Bloland, H. (1997) *"The Role Of Associations in the Professionalizing Process"*, New Directions for Philanthropic Fundraising, Vol. 15, pp.97–110.
- Bodin, L., Gordon, L. and Loeb, M. (2008) *"Information Security and Risk Management"*, Communications of the ACM, Vol. 51, No. 4, pp.64–68.
- Bond, P. (1975) *"The Forever Changing DP Department"*, Computer Weekly, April 17th, 1975.
- Bonner, W. and Chiasson, M. (2005) *"If Fair Information Principles Are the Answer, What Was the Question? An Actor–Network Theory Investigation of the Modern Constitution of Privacy"*, Information and Organization, Vol. 15, No. 4, pp.267–293.
- Boss, S., Kirsch, L., Angermeier, I., Shingler, R. and Boss, W. (2009) *"If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security"*, European Journal of Information Systems, Vol. 18, No. 2, pp.151–164.
- Bowen-Schire, M., Reid, B., Ezingear, J.-N. and Birchall, D. (2004) *"Identity Management and Power in the Discourse of Information Security Managers"*, 6th International Conference on Organizational Discourse, Amsterdam 2004.
- Brady, S. (2007a) *"The Maturity of IT Professionalism in Europe"*, Upgrade, Vol. 8, No. 1, pp.59–67.
- Brady, S. (2007b) *"Professionalising the IT Industry: Towards the Creation of a Professional Association"*, Unpublished D.Prof. Thesis, Middlesex University.
- Brante, T. (2011) *"Professions as Science-Based Occupations"*, Professions and Professionalism, Vol. 1, No. 1, pp.4–20.
- British Broadcasting Corporation [BBC] (2011) *"Fake DigiNotar Web Certificate Risk to Iranians"* [online], Available at: <<http://www.bbc.co.uk/news/technology-14789763>> [Accessed 10/09/2011].
- Brocaglia, J. (2005) *"The Information Security Officer: A New Role for New Threats"*, IN: Green, E. (Ed.) *"The Black Book on Corporate Security"*, 2nd Edition, Potomac: Larstan Publishing.
- Brock, D. (2016) *"Professionals and Their Workplaces in Emerging Markets– A Research Agenda"*, International Journal of Emerging Markets, Vol. 11, No. 3, pp.460–472.
- Broderick, J. (2006) *"ISMS, Security Standards and Security Regulations"*, Information Security Technical Report, Vol. 11, pp.26–31.
- Brooks, L. and Atkinson, C. (2004) *"StructurANTion in Research and Practice: Representing Actor Networks Their Structurated Orders and Translations"*, IN: Kaplan, B., Truex, D., Wastell, D., Wood-Harper, T. and DeGross, J. (Eds.) *"Information Systems Research: Relevant Theory and Informed Practice"*, Boston: Kluwer Academic Publishers, pp.389–409.
- Brotby, K. (2009) *"Information Security Governance"*, Chichester: John Wiley and Sons.
- Buche, M. and Vician, C. (2005) *"A Unified Information Security Management Plan"*, IN: Nemati, H. (Ed.) *"Information Security and Ethics: Concepts, Methodologies, Tools, and Applications"*, Vol. 1, Hershey: Idea Group.

- Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) *"Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness"*, Management Information Systems Quarterly, Vol. 34, No. 3, pp.523–548.
- Bunker, G. (2012) *"Technology is Not Enough: Taking a Holistic View for Information Assurance"*, Information Security Technical Report, Vol. 17, pp.19–25.
- Burdon, M., Siganto, J. and Coles-Kemp, L. (2016) *"The Regulatory Challenges of Australian Information Security Practice"*, Computers and Security, Vol. 32, pp.623–633.
- Burley, D., Eisenberg, J. and Goodman, S. (2014) *"Would Cybersecurity Professionalization Help Address the Cybersecurity Crisis?"*, Communications of the ACM, Vol. 57, No. 2, pp.24–27.
- Burrell, G. and Morgan, G. (1979) *"Sociological Paradigms and Organisational Analysis"*, Farnham: Ashgate.
- Calder, A. and Watkins, S. (2008) *"A Manager's Guide to Data Security & ISO27001/ISO27002"*, 4th Edition, London: Kogan Page.
- Callon, M. (1986) *"Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay"*, IN: Law, J. (Ed.) *"Power, Action and Belief: A New Sociology of Knowledge"*, London: Sociological Review Monograph.
- Callon, M. (1999) *"Actor–Network Theory– The Market Test"*, IN: Law, J. and Hassard, J. (Eds.) *"Actor Network Theory and After"*, Oxford: Blackwell.
- Callon, M. and Latour, B. (1981) *"Unscrewing the Big Leviathan: How Actors Macro-Structure Reality and How Sociologists Help Them to Do So"*, IN: Knorr-Cetina, K. and Cicourel, A. (Eds.) *"Advances in Social Theory and Methodology: Toward an Integration of Micro- and Macro-Sociologies"*, Abingdon: Routledge, pp.277–303.
- Callon, M. and Latour, B. (1992) *"Don't Throw the Baby Out With the Bath School! A Reply to Collins and Yearley"*, IN: Pickering, A. (Ed.) *"Science as Practice and Culture"*, Chicago: University of Chicago Press, pp.343–368.
- Campbell, K., Gordon, L., Loeb, M. and Zhou, L. (2003) *"The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market"*, Journal of Computer Security, Vol. 11, pp.431–448.
- Cannoy, S., Palvia, P. and Schilhavy, R. (2006) *"A Research Framework for Information Systems Security"*, Journal of Information Privacy and Security, Vol. 2, No. 2, pp.3–29.
- Carcary, M., Renaud, K., McLaughlin, S. and O'Brien, C. (2016) *"A Framework for Information Security Governance and Management"*, IT Professional, Vol. 18, No. 2, pp.22–30.
- Carr-Saunders, A. and Wilson, P. (1933) *"The Professions"*, London: Birchall.
- Cavusoglu, H., Cavusoglu, H., Son, J.-Y. and Benbasat, I. (2015) *"Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security"*

Control Resources", Information and Management, Vol. 52, pp.385–400.

Cepeda, G. and Martin, D. (2005) "A Review of Case Studies Publishing in Management Decision: Guides and Criteria for Achieving Quality in Qualitative Research", Management Decision, Vol. 43, No. 6, pp.851–876.

Cho, S., Mathiassen, L. and Nilsson, A. (2008) "Contextual Dynamics During Health Information Systems Implementation: An Event-Based Actor–Network Approach", European Journal of Information Systems, No. 17, pp.614–630.

Christmas, P. (1992) "Network Security Manager", London: Elseiver.

Chua, W. (1986) "Radical Developments in Accounting Thought", The Accounting Review, Vol. 61, No. 4, pp.601–632.

Chun, M. and Mooney, J. (2009) "CIO Roles and Responsibilities: Twenty-Five Years of Evolution and Change", Information and Management, Vol. 46, pp.323–334.

Clark, C. (2005) "The Deprofessionalisation Thesis, Accountability and Professional Character", Social Work and Society, Vol. 3, No. 2, pp.182–190.

Cogan, M. (1955) "The Problem of Defining a Profession", The Annals of the American Academy of Political and Social Science, Vol. 297, pp.105–111.

Coles-Kemp, L. (2009) "Information Security Management: An Entangled Research Challenge", Information Security Technical Report, Vol. 14, pp.181–185.

Colley, J. (2008) "Managing Both Careers and Risks", Network Security, No. 5, pp.7–9.

Collins, H. and Yearley, S. (1992) "Epistemological Chicken", IN: Pickering, A. (Ed.) "Science as Practice and Culture", Chicago: University of Chicago Press, pp.301–326.

Collins, R. (1990) "Changing Conceptions in the Sociology of the Professions", IN: Torstendahl, R. and Burrage, M. (Eds.) "The Formation of the Professions", London: Sage, pp.11–23.

Colloquium for Information Systems Security Education (2016) "About CISSE" [online], Available at: <<http://www.cisse.info/about>> [Accessed 13/06/2013].

Communications Electronics Security Group [CESG] (2012a) "CESG Certification for IA Professionals", Issue 2.0, Cheltenham: CESG.

Communications Electronics Security Group [CESG] (2012b) "Guidance to CESG Certification for IA Professionals", Issue 1.0, Cheltenham: CESG.

Communications Electronics Security Group [CESG] (2015) "The Problems With Forcing Regular Password Expiry" [online], Available at: <https://www.cesg.gov.uk/content/files/document_files/Password_guidance_-_simplifying_your_approach_back_cover.pdf> [Accessed 16/07/16].

Communications Electronics Security Group [CESG] (2016) "GCHQ Certification of Bachelor's Degrees in Cyber Security" [online], Available at: <<https://www.cesg.gov.uk/articles/gchq-certification-bachelors-degrees-cyber-security>> [Accessed 07/07/2016].

- Coole, M., Brooks, D. and Treagust, D. (2015) *"The Physical Security Professional: Formulating a Novel Body of Knowledge"*, Journal of Applied Security Research, Vol. 10, pp.385–410.
- Cordella, A. and Shaikh, M. (2006) *"From Epistemology to Ontology: Challenging the Constructed 'Truth' of ANT"*, Working Paper Series: Department of Information Systems, London School of Economics and Political Science.
- Courtney, R. (1977) *"Security Risk Assessment in Electronic Data Processing Systems"*, IN: *"Proceedings of the National Computer Conference (AFIPS '77)"*, June 13–16, 1977, New York: ACM, pp.97–104.
- Cresson-Wood, C. (1997) *"Information Security Staffing Levels and the Standard of Due Care"*, Computer Fraud and Security, No. 4, pp.8–9.
- Cresswell, J. (2009) *"Research Design: Qualitative, Quantitative and Mixed Approaches"*, London: Sage.
- Crook, D. (2008) *"Some Historical Perspectives on Professionalism"*, IN: Cunningham, B. (Ed.) *"Exploring Professionalism"*, London: Institute of Education, University of London, pp.10–27.
- Crossler, R., Johnston, A., Lowry, P., Hud, Q., Warkentin, M. and Baskerville, R. (2013) *"Future Directions for Behavioral Information Security Research"*, Computers and Security, Vol. 32, pp.90–101.
- Currie, G., Koteyko, N. and Nerlich, B. (2009) *"The Dynamics of Professions and Development of New Roles in Public Services Organizations: The Case of Modern Matrons in the English NHS"*, Public Administration, Vol. 87, No. 2, pp.295–311.
- D'Arcy, J., Hovav, A. and Galletta, D. (2009) *"User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach"*, Information Systems Research, Vol. 20, No. 1, pp.79–98.
- Da Veiga, A. and Eloff, J. (2007) *"An Information Security Governance Framework"*, Information Systems Management, Vol. 24, pp.361–372.
- Da Veiga, A. and Eloff, J. (2010) *"A Framework and Assessment Instrument for Information Security Culture"*, Computers and Security, Vol. 29, pp.196–207.
- Davis, R. (2011) *"Advancing Nursing Jurisdiction in Diabetes Care"*, Unpublished Ph.D. Thesis, University of Glamorgan.
- De Leeuw, K. (2007) *"Introduction"* IN: De Leeuw, K. and Bergstra, J. (Eds.) *"The History of Information Security"*, London: Elsevier.
- De Nardis, L. (2007) *"A History of Internet Security"* IN: De Leeuw, K. and Bergstra, J. (Eds.) *"The History of Information Security"*, London: Elsevier.
- Delattre, M. and Ocler, R. (2013) *"Professionalism and Organization: Polysemy of Concepts and Narratives of Actors"*, Society and Business Review, Vol. 8, No. 1, pp.18–31.
- Department for Business, Enterprise and Regulatory Reform [BERR] (2008) *"BERR Information Security Breaches Survey 2008"* [online], Available at: <http://www.pwc.co.uk/eng/publications/berr_information

_security_breaches_survey_2008.html> [Accessed 13/08/2011].

Department for Business, Innovation and Skills [DBIS] (2012) "*Business Populations Estimates for the UK and Regions, 2012 (Methodology Note)*" [online], Available at: <"http://www.bis.gov.uk/analysis/statistics/business-population-estimates"> [Accessed 24/11/2012].

Department for Business, Innovation and Skills [DBIS] (2014a) "*Cyber Security Skills: Business Perspectives and Government's Next Steps*", London: HMSO.

Department for Business, Innovation and Skills [DBIS] (2014b) "*Cyber Security Skills: Business Perspectives and Government's Next Steps (Supporting Evidence)*", London: HMSO.

Department for Culture, Media and Sport [DCMS] (2016) "*Developing Our Capability in Cyber Security: Academic Centres of Excellence in Cyber Security Research*" [online], Accessible at: <https://www.gov.uk/government/publications/cyber-security-research-capability-academic-centres-of-excellence> [Accessed 18/06/2016].

Department of Trade and Industry [DTI] (2004) "*Information Security Breaches Survey 2004*" [online], Available at: <http://www.pwc.co.uk/pdf/dti_technical_report_2004.pdf> [Accessed 17/09/2011].

Dery, K., Hall, R., Wailes, N. and Wiblen, S. (2013) "*Lost in Translation? An Actor–Network Approach to HRIS Implementation*", Journal of Strategic Information Systems, Vol. 22, No. 3, pp.225–237.

Dhillon, G. (1995) "*Interpreting the Management of Information Systems Security*", Unpublished Ph.D. Thesis, University of London.

Dhillon, G. (1997) "*Managing Information System Security*", London: Macmillan.

Dhillon, G. and Backhouse, J. (2000) "*Technical Opinion: Information System Security Management in the New Millennium*", Communications of the ACM, Vol. 43, No. 7, pp.125–128.

Dhillon, G. and Backhouse, J. (2001) "*Current Directions in IS Security Research: Towards Socio-Organizational Perspectives*", Information Systems Journal, Vol. 11, pp. 127–153.

Dhillon, G. and Mishra, S. (2008) "*The Impact of Sarbanes–Oxley (SOX) Act on Information Security Governance*", IN: Nemati, H. (Ed.) "*Information Security and Ethics: Concepts, Methodologies, Tools, and Applications*", Vol. IV, New York: Hershey, pp.2545–2559.

Dhillon, G. and Torkzadeh, G. (2006) "*Value-Focused Assessment of Information System Security in Organizations*", Information Systems Journal, Vol. 16, pp.293–314.

Dhillon, G., Oliveira, S., Susarapu, S. and Caldeira, M. (2016) "*Deciding Between Information Security and Usability: Developing Value Based Objectives*", Computers in Human Behaviour, Vol. 61, pp.656–666.

Díaz Andrade, A. and Urquhart, C. (2010) "*The Affordances of Actor Network Theory in ICT for Development Research*", Information Technology and People, Vol. 23, No. 4, pp.352–374.

DiMaggio, P. and Powell, W. (1983) "*The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*", American Sociological Review, Vol. 48, No. 2, pp.147–160.

- Dlamini, M., Eloff, J. and Eloff, M. (2009) *"Information Security: The Moving Target"*, Computers and Security, Vol. 28, pp.189–198.
- Doherty, N. and Fulford, H. (2005) *"Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis"*, Information Resources Management Journal, Vol. 18, No. 4, pp.21–38.
- Doherty, N. and Fulford, H. (2006) *"Aligning the Information Security Policy with the Strategic Information Systems Plan"*, Computers and Security, Vol. 25, pp.55–63.
- Doolin, B. and Lowe, A. (2002) *"To Reveal is To Critique: Actor–Network Theory and Critical Information Systems Research"*, Journal of Information Technology, Vol. 17, pp.69–78.
- Downie, R. (1990) *"Professions and Professionalism"*, Journal of Philosophy of Education, Vol. 24, No. 2, pp.147–159.
- Drever, E. (2003) *"Using Semi-Structured Interviews in Small-Scale Research"*, Revised Edition, Glasgow: SCRE Centre, University of Glasgow.
- Dyer, O. (2008) *"UK Tightens Rules on Cannabis Despite Advice Not Do to So"*, British Medical Journal, Vol. 336, No. 7653, p.1095.
- E-Skills UK (2013) *"Career Analysis into Cyber Security: New & Evolving Occupations"*, London: E-Skills UK.
- Ehrenreich, B. and Ehrenreich, J. (1979) *"The Professional–Managerial Class"*, IN: Walker, P. (Ed.) *"Between Labor and Capital"*, Boston: South End Press, pp.5–45.
- Eisikovits, Z. and Koren, C. (2010) *"Approaches to and Outcomes of Dyadic Interview Analysis"*, Qualitative Health Research, Vol. 20, No. 12, pp.1642–1655.
- Elder-Vass, D. (2015) *"Disassembling Actor–Network Theory"*, Philosophy of the Social Sciences, Vol. 45, No. 1, pp.100–121.
- Eloff, J. and Eloff, M. (2003) *"Information Security Management – A New Paradigm"*, IN: *"Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement Through Technology"*, SAICSIT '03, pp.130–136.
- Elzinga, A. (1990) *"The Knowledge Aspect of Professionalization: The Case of Science-Based Nursing Education in Sweden"*, IN: Torstendahl, R. and Burrage, M. (Eds.) *"The Formation of the Professions"*, London: Sage, pp.11–23.
- Ensor, C. (2016) *"Investing in UK Cyber"*, ITNow, June 2016, pp.58–59.
- Everett, C. (2009) *"Professionalism: The Old Versus the New"*, Computer Fraud and Security, No. 3, pp.5–6.
- Everett, C. (2011) *"The Slow Road to Professionalisation"*, Computer Fraud and Security, No. 4, pp.9–11.
- Evetts, J. (2003) *"The Sociological Analysis of Professionalism: Occupational Change in the Modern*

World", International Sociology, Vol. 18, pp.395–415.

Evetts, J. (2006) *"Short Note: The Sociology of Professional Groups: New Directions"*, Current Sociology, Vol. 54, No. 1, pp.133–143.

Evetts, J. (2013) *"Professionalism: Value and Ideology"*, Current Sociology Review, Vol. 61, Nos. 5–6, pp.778–796.

Ezingear, J.-N. and Bowen-Schrire, M. (2007) *"Triggers of Change in Information Security Management Practices"*, Journal of General Management, Vol. 32, No. 4, pp.53–72.

Fairweather, N. (2004) *"NO, PAPA"*, IN: Bynum, T. and Rogerson, S. (Eds.) *"Computer Ethics and Professional Responsibility"*, Oxford: Blackwell, pp.148–156.

Faulconbridge, J. and Muzio, D. (2012) *"The Rescaling of the Professions: Towards a Transnational Sociology of the Professions"*, International Sociology, Vol. 27, No. 1, pp.109–125.

Fink, D., Huegle, T. and Dortschy, M. (2008) *"A Model of Information Security Governance for E-Business"*, IN: Nemati, H. (Ed.) *"Information Security and Ethics: Concepts, Methodologies, Tools, and Applications"*, Vol. IV, New York: Hershey, pp.2958–2967.

Fitzgerald, T. (2007) *"Clarifying the Roles of Information Security: 13 Questions the CEO, CIO and CISO Must Ask Each Other"*, Information Systems Security, Vol. 16, No. 5, pp.257–263.

Flick, U. (2009) *"An Introduction to Qualitative Research"*, 4th Edition, London: Sage.

Flowerday, S. and Tuyikeze, T. (2016) *"Information Security Policy Development and Implementation: The What, How and Who"*, Computers and Security, Vol. 61, pp.169–183.

Foddy, W. (1993) *"Constructing Questions for Interviews and Questionnaires"*, Cambridge: Cambridge University Press.

Foster, S. (2005) *"Building a Secure Corporate Environment"*, IN: Green, E. (Ed.) *"The Black Book on Corporate Security"*, 2nd Edition, Potomac: Larstan Publishing.

Fournier, V. (1999) *"The Appeal to 'Professionalism' as a Disciplinary Mechanism"*, Social Review, Vol. 47, No. 2, pp.280–307.

Frangopoulos, E., Eloff, M. and Venter, L. (2013) *"Psychosocial Risks: Can Their Effects on the Security of Information Systems Really Be Ignored?"*, Information Management and Computer Security, Vol. 21, pp.53–65.

Freeman, E. (2007) *"Regulatory Compliance and the Chief Compliance Officer"*, Information Systems Security, Vol. 16, pp.357–361.

Freidson, E. (1970) *"Profession of Medicine: A Study of the Sociology of Applied Knowledge"*, Chicago: University of Chicago Press.

Freidson, E. (1973) *"Professionalization and the Organization of Middle-Class Labour in Post-Industrial Society"*, IN: Halmos, P. (Ed.) *"Professionalisation and Social Change"*, Keele: University of Keele, pp.47–59.

- Freidson, E. (1986) *"Professional Powers: A Study of the Institutionalization of Formal Knowledge"*, Chicago: University of Chicago Press.
- Freidson, E. (1988) *"Profession of Medicine: A Study of the Sociology of Applied Knowledge (With a New Afterword)"*, Chicago: University of Chicago Press.
- Freidson, E. (1994) *"Professionalism Reborn: Theory, Prophecy and Policy"*, Oxford: Polity Press.
- Freidson, E. (2001) *"Professionalism: The Third Logic"*, Chicago: University of Chicago Press.
- Frinke, D. and Bishop, M. (2004) *"Joining the Security Education Community"*, IEEE Security and Privacy, Vol. 2, No. 5, pp.61–63.
- Frost & Sullivan and (ISC)² (2015a) *"The 2015 (ISC)² Global Information Workforce Study"* [online, protected], Available at: < <https://www.isc2.org> > [Accessed 12/06/2016].
- Frost & Sullivan and (ISC)² (2015b) *"Women in Security: Wisely Positioned for the Future of InfoSec"* [online], Available at: <<https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/2015-Women-In-Security-Study.pdf>> [Accessed: 12/6/2016].
- Fuchs, L., Pernul, G. and Sandhu, R. (2011) *"Roles in Information Security – A Survey and Classification of the Research Area"*, Computers and Security, Vol. 30, pp.748–769.
- Fulford, H. and Doherty, N. (2003) *"The Application of Information Security Policies in Large UK-Based Organizations: An Exploratory Investigation"*, Information Management and Computer Security, Vol. 11, No. 3, pp.106–114.
- Furnell, S. (2004) *"Qualified to Help: In Search of the Skills to Ensure Security"*, Computer Fraud and Security, Vol. 12, pp.10–14.
- Furnell, S. and Clarke, N. (2012) *"Power to the People? The Evolving Recognition of Human Aspects of Security"*, Computers and Security, Vol. 31, pp.983–988.
- Furnell, S. and Thomson, K.-L. (2009) *"From Culture to Disobedience: Recognising the Varying User Acceptance of IT Security"*, Computer Fraud and Security, No. 2, pp.5–10.
- Fletcher, L., Schroder, C. and von Solms, R. (2010) *"Information Security Education in South Africa"*, Information Management and Computer Security, Vol. 18, No. 5, pp.366–374.
- Gad, C. and Jensen, C. (2010) *"On the Consequences of Post-ANT"*, Science, Technology and Human Values, Vol. 35, No. 1, pp.55–80.
- Galliers, R. and Land, F. (2002) *"Choosing Appropriate Information Systems Research Methodologies"*, IN: Myers, M. and Avison, D. (Eds.) *"Qualitative Research in Information Systems: A Reader"*, London: Sage.
- Gerber, M. and von Solms, R. (2001) *"From Risk Analysis to Security Requirements"*, Computers and Security, Vol. 20, No. 7, pp.577–584.
- Gerber, M. and von Solms, R. (2008) *"Information Security Requirements – Interpreting the Legal Aspects"*, Computers and Security, Vol. 27, No.5, pp.124–135.

- Gibbs, G. (2007) *"Analysing Qualitative Data"*, London: Sage.
- Gilmore, S. and Williams, S. (2007) *"Conceptualising the 'Personnel Professional': A Critical Analysis of the Chartered Institute of Personnel and Development's Professional Qualification Scheme"*, *Personnel Review*, Vol. 36, No. 3, pp.398–414.
- Glaser, B. and Strauss, A. (1967) *"The Discovery of Grounded Theory"*, New York: Aldine De Gruyter.
- Gollman, D. (2011) *"Computer Security"*, 3rd Edition, John Wiley and Sons.
- Gonzales, G. and Cox, A. (2010) *"Implementing a Human Resources Competency-Based Model: An Actor–Network Perspective"*, *Proceedings of the Sixteenth Americas Conference on Information Systems*, August 12–15, 2010, Lima, Peru.
- Goode, W. (1960) *"The Profession: Reports and Opinion. Encroachment, Charlatanism, and the Emerging Profession: Psychology, Sociology, and Medicine"*, *American Sociological Review*, Vol. 25, No. 6, pp.902–965.
- Gordon, L. and Loeb, M. (2002) *"The Economics of Information Security Investment"*, *ACM Transactions on Information and System Security*, Vol. 5, No. 4, pp.438–457.
- Gordon, L., Loeb, M. and Lucyshyn, W. (2003a) *"Sharing Information on Computer Systems Security: An Economic Analysis"*, *Journal of Accounting and Public Policy*, Vol. 22, No. 6, pp.461–485.
- Gordon, L., Loeb, M. and Lucyshyn, W. (2003b) *"Information Security Expenditures and Real Options: A Wait-and-See Approach"*, *Computer Security Journal*, Vol. 19, No. 2, pp.1–7.
- Gorman, E. and Sandefur, R. (2011) *"'Golden Age', Quiescence, and Revival: How the Sociology of Professions Became the Study of Knowledge-Based Work"*, *Work and Occupations* Vol. 38, pp.275–303.
- Gotterbarn, D. (2004) *"On Licensing Computer Professionals"*, IN: Bynum, T. and Rogerson, S. (Eds.) *"Computer Ethics and Professional Responsibility"*, Oxford: Blackwell, pp.157–201.
- Government Communications Headquarters [GCHQ] (2016) *"GCHQ Certification of Cyber Security Training Courses, Version 2.0"* [online], Available at: <https://www.cesg.gov.uk/content/files/protected_files/document_files/GCT%20scheme%20-%20Course%20Content%20Criteria%20v2%200.pdf> [Accessed 13/06/2016].
- Grandison, T., and Bhatti, R. (2010) *"HIPAA Compliance and Patient Privacy Protection"*, *Studies in Health Technology and Informatics*, Vol. 160, No. 1, pp.884–888.
- Graneheim, U. and Lundman, B. (2004) *"Qualitative Content Analysis in Nursing Research: Concepts, Procedures and Measures to Achieve Trustworthiness"*, *Nurse Education Today*, Vol. 24, No. 2, pp.105–112.
- Greenwald, S. (1998) *"Discussion Topic: What is the Old Security Paradigm?"* IN: *"Proceedings of the 1998 Workshop on New Security Paradigms"*, September 22–25, 1998, Charlottesville: ACM, pp.107–118.
- Greenwood, E. (1957) *"Attributes of a Profession"*, *Social Work*, Vol. 2, No. 3, pp.45–55.
- Greenwood, R., Suddaby, R. and Hinings, C. (2002) *"Theorizing Change: The Role of Professional*

Associations in the Transformation of Institutional Fields", Academy of Management Journal, Vol. 45, No. 1, pp.58–80.

Gregor, S. (2006) *"The Nature of Theory in Information Systems"*, Management Information Systems Quarterly, Vol. 30, No. 3, pp.611–642.

Griffiths, M., Brooks, D. and Corkill, J. (2010) *"Defining the Security Professional: Definition through a Body of Knowledge"*, IN: *"Proceedings of the 3rd Australian Security and Intelligence Conference"*, Edith Cowan University, Perth Western Australia, 30th November – 2nd December, 2010, pp.44–52.

Guo, K. (2013) *"Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis"*, Computers and Security, Vol. 32, pp.242–251.

Guzman, I., Stam, K. and Stanton, J. (2008) *"The Occupational Culture of IS/IT Personnel within Organisations"*, The Database for Advances in Information Systems, Vol. 39, No. 1, pp.33–50.

Guzman, I., Stanton, J., Stam, K., Vijayasri, V., Yamodo, I., Zakaria, N. and Caldera, C. (2004) *"A Qualitative Study of the Occupational Subculture of Information Systems Employees in Organizations,"* IN: *"Proceedings of the 2004 SIGMIS Conference on Computer Personnel Research: Careers, Culture and Ethics in a Networked Environment"*, New York: ACM, pp.74–80.

Hall, R. (1968) *"Professionalization and Bureaucratization"*, American Sociological Review, Vol. 33, No. 1, pp.92–104.

Hanlon, G. (1998) *"Professionalism as Enterprise: Service Class Politics and the Redefinition of Professionalism"*, Sociology, Vol. 32, No. 1, pp.43–63.

Harvey, L. and Myers, M. (2002) *"Scholarship and Practice: The Contribution of Ethnographic Research Methods to Bridging the Gap"*, IN: Myers, M. and Avison, D. (Eds.) *"Qualitative Research in Information Systems: A Reader"*, London: Sage, pp.13–27.

Hayes, M. (2002) *"Where The Chief Security Officer Belongs"*, InformationWeek, Feb 25, 2002, [online], Available at <<http://www.informationweek.com/news/6500913>> [Accessed 28/05/2011].

Hedström, K., Dhillon, H. and Karlsson, F. (2010) *"Using Actor Network Theory to Understand Information Security Management"*, IN: Rannenberg, K., Varadharajan, V. and Weber, C. (Eds.) *"Security and Privacy – Silver Linings in the Cloud"*, Proceedings of the 25th IFIP TC-11 International Information Security Conference, SEC 2010 (WCC 2010), Brisbane, Australia, September 20–23, 2010, pp.43–54.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J. (2011) *"Value Conflicts for Information Security Management"*, The Journal of Strategic Information Systems, Vol. 20, No. 4, pp.373–384.

Heinrich, T. (2013) *"Standard Wars, Tied Standards, and Network Externality Induced Path Dependence in the ICT Sector"*, Technological Forecasting and Social Change, Vol. 81, pp.309–320.

Hentea, M., Dhillon, H. and Dhillon, M. (2006) *"Towards Changes in Information Security Education"*, Journal of Information Technology Education, Vol. 5, pp.221–232.

Herath, T. and Rao, H. (2009a) *"Encouraging Information Security Behaviors in Organizations: Role of*

Penalties, Pressures and Perceived Effectiveness", Decision Support Systems, Vol. 47, pp.154–165.

Herath, T. and Rao, H. (2009b) *"Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations"*, European Journal of Information Systems, Vol. 18, pp.106–125.

Hitchings, J. (1995) *"Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology"*, Computers and Security, Vol. 14, pp.377–383.

Hoffman, L., Burley, D. and Toregas, C. (2012) *"Holistically Building the Cybersecurity Workforce"*, IEEE Security and Privacy, Vol. 10, No. 2, pp.33–39.

Holden, M. and Lynch, P. (2004) *"Choosing the Appropriate Methodology: Understanding Research Philosophy"*, Marketing Review, Vol. 4, No. 4, pp.397–409.

Hollis, M. (1994) *"The Philosophy of Social Science"*, Revised Edition, Cambridge: Cambridge University Press.

Höne, K. and Eloff, J. (2002a) *"Information Security Policy – What Do International Information Security Standards Say?"*, Computers and Security, Vol. 21, No. 5, pp.402–409.

Höne, K. and Eloff, J. (2002b) *"What Makes an Effective Information Security Policy?"*, Network Security, No. 6, pp.14–16.

Horrocks, I. (2001) *"Security Training: Education for an Emerging Profession?"*, Computers and Security, Vol. 20, No. 3, pp.219–226.

Hovav, A. and D'Arcy, J. (2003) *"The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms"*, Risk Management and Insurance Review, Vol. 6, No. 2, pp.97–121.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012) *"Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture"*, Decision Sciences, Vol. 43, No. 4, pp.615–660.

Humphreys, E. (2008) *"Information Security Management Standards: Compliance, Governance and Risk Management"*, Information Security Technical Report, Vol. 13, pp.247–255.

Ifinedo, P. (2014) *"Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition"*, Information and Management, Vol. 51, pp. 69–79.

Illich, I. (1977) *"Disabling Professions"*, IN: Illich, I., Zola, I. and McKnight, J. (Eds.) *"Disabling Professions"*, London: Marion Boyars.

Introna, L. and Ilharco, F. (2004) *"Phenomenology, Screens and the World: A Journey with Husserl and Heidegger into Phenomenology"*, IN: Mingers, J. and Willcocks, L. (Eds.) *"Social Theory and Philosophy for Information Systems"*, Chichester: John Wiley and Sons.

Irons, A., Savage, N., Maple, C., Davies, A. and Turley, L. (2016) *"Cybersecurity in CS Degrees"*, ITNow, June 2016, pp.56–57.

(ISC)² and CPHC (2015) *"Cybersecurity Principles and Learning Outcomes for Computer Science and IT-Related Degrees"*, Version 1.1, July 2015.

- Jick, T. (1979) *"Mixing Qualitative and Quantitative Methods: Triangulation in Action"*, Administrative Science Quarterly, Vol. 24, No. 4, pp.602–611.
- Johnson, M. and Goetz, E. (2007) *"Embedding Information Security into the Organization"*, IEEE Security and Privacy, Vol. 5, No. 3, pp.16–24.
- Johnson, M., Goetz, E. and Pflieger, S. (2009) *"Security Through Information Risk Management"*, IEEE Security and Privacy, Vol. 7, No. 3, pp.45–52.
- Johnson, T. (1972) *"Professions and Power"*, London: Macmillan.
- Johnston, R. (2001) *"Situated Action, Structuration and Actor–Network Theory: An Integrative Theoretical Perspective"*, IN: *"Global Co-Operation in the New Millennium"*, Proceedings of ECIS 2001: 9th European Conference on Information Systems, Bled, Slovenia, June 27–29, 2001.
- Jones, M., Orlikowski, W. and Munir, K. (2004) *"Structuration Theory and Information Systems: A Critical Reappraisal"*, IN: Mingers, J. and Willcocks, L. (Eds.) *"Social Theory and Philosophy for Information Systems"*, Chichester: John Wiley and Sons.
- Kahn, D. (1974) *"The Codebreakers"*, Abridged Edition, New York: Macmillan.
- Kahn, R., Wolfe, D., Quinn, R., Snoek, J. and Rosenthal, R. (1964) *"Organizational Stress: Studies in Role Conflict and Ambiguity"*, Oxford: John Wiley.
- Kandogan, E. and Haber, E. (2005) *"Security Administration Tools and Practices"*, IN: Cranor, L. and Garfinkel, S. (Eds.) *"Security and Usability: Designing Secure Systems that People Can Use"*, Sebastopol: O'Reilly, pp.374–394.
- Kankanhalli, A., Teo, H.-H., Tan, B. and Wei, K.-K. (2003) *"An Integrative Study of Information Systems Security Effectiveness"*, International Journal of Information Management, Vol. 23, pp.139–154.
- Karlsson, F., Åström, J. and Karlsson, M. (2015) *"Information Security Culture– State-of-the-Art Review Between 2000 and 2013"*, Information and Computer Security, Vol. 23, No. 3, pp.246–285.
- Katz, M. and Shapiro, C. (1994) *"Systems Competition and Network Effects"*, Journal of Economic Perspectives, Vol. 8, No. 2, pp.93–115.
- Kayworth, T. and Whitten, D. (2010) *"Effective Information Security Requires a Balance of Social and Technology Factors"*, Management Information Systems Quarterly Executive, Vol. 9, No. 3, pp.163–175.
- Kitchener, M. (2000) *"The 'Bureaucratization' of Professional Roles: The Case of Clinical Directors in UK Hospitals"*, Organization, Vol.7, No. 1, pp.129–154.
- Kitzinger, J. (1995) *"Introducing Focus Groups"*, British Medical Journal, Vol. 311, pp.299–302.
- Klein, H. and Huynh, M. (2004) *"The Critical Social Theory of Jürgen Habermas and Its Implications for IS Research"*, IN: Mingers, J. and Willcocks, L. (Eds.) *"Social Theory and Philosophy for Information Systems"*, Chichester: John Wiley and Sons.
- Klein, H. and Myers, M. (1999) *"A Set of Principles for Conducting and Evaluating Interpretative Field Studies in Information Systems"*, Management Information Systems Quarterly, Vol. 23, No. 1, pp.67–93.

- Knapp, K., Marshall, T., Rainer, R. and Ford, F. (2006) *"Information Security: Management's Effect on Culture and Policy"*, Information Management and Computer Security, Vol. 14, No. 1, pp.24–36.
- Knowles, W., Baron, A. and McGarr, T. (2016) *"The Simulated Security Assessment Ecosystem: Does Penetration Testing Need Standardisation?"*, Computers and Security, Vol. 62, pp.296–316.
- Kolkowska, E. and Dhillon, G. (2013) *"Organizational Power and Information Security Rule Compliance"*, Computers and Security, Vol. 33, pp.3–11.
- Komatsu, A., Takagi, D. and Takemura, T. (2013) *"Human Aspects of Information Security: An Empirical Study of Intentional Versus Actual Behavior"*, Information Management and Computer Security, Vol. 21, No.1, pp.5–15.
- Konstantinou, E. (2015) *"Professionalism in Project Management: Redefining the Role of the Project Practitioner"*, Project Management Journal, Vol. 46, No. 2, pp.21–35.
- Kotulic, A. and Clark, J. (2004) *"Why There Aren't More Information Security Research Studies"*, Information and Management, Vol. 41, pp.597–603.
- Kraemer, S., Carayon, P. and Clem, J. (2009) *"Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities"*, Computers and Security, Vol. 28, No. 7, pp.509–520.
- Kuhn, T. (1970) *"The Structure of Scientific Revolutions"*, Enlarged (2nd ed.), Chicago: University of Chicago Press.
- Lacey, D. (2006) *"A New Institute for a New Millennium"*, Information Security Technical Report, Vol. 11, pp.62–65.
- Lamb, R. and Kling, R. (2003) *"Reconceptualizing Users as Social Actors in Information Systems Research"*, Management Information Systems Quarterly, Vol. 27, No. 2, pp.197–236.
- Larson, M. (1977) *"The Rise of Professionalism: A Sociological Analysis"*, Berkeley: University of California Press.
- Larson, M. (2013) *"The Rise of Professionalism: Monopolies of Competence and Sheltered Markets [New Introduction by the Author]"*, New Brunswick: Transaction Publishers.
- Latour, B. (1987) *"Science in Action: How to Follow Scientists and Engineers Through Society"*, Milton Keynes: Oxford University Press.
- Latour, B. (1988) *"The Pasteurization of France"*, Harvard: Harvard University Press.
- Latour, B. (1991) *"Technology is Society Made Durable"*, IN: Law, J. (Ed.) *"A Sociology of Monsters: Essays on Power, Technology and Domination"*, London: Routledge, pp.103–131.
- Latour, B. (1999a) *"On Recalling ANT"*, The Sociological Review, Vol. 47, No. S1, pp.15–25.
- Latour, B. (1999b) *"Pandora's Hope. An Essay on the Reality of Science Studies"*, Cambridge: Harvard University Press.
- Latour, B. (2005) *"Reassembling the Social"*, Oxford: Oxford University Press.

- Law, J. (1986) "*Editor's Introduction: Power/Knowledge and the Dissolution of the Sociology of Knowledge*", IN: Law, J. (Ed.) "*Power, Action and Belief: A New Sociology of Knowledge*", London: Sociological Review Monograph.
- Law, J. (1992) "*Notes on the Theory of the Actor–Network: Ordering, Strategy and Heterogeneity*", *Systems Practice*, Vol. 5, pp.379–93.
- Lee, A. (1989) "*A Scientific Methodology for MIS Case Studies*", *Management Information Systems Quarterly*, Vol. 13, No. 1, pp.33–50.
- Lee, A. (2001) "*Editor's Comments*", *Management Information Systems Quarterly*, Vol. 24, No. 1, pp.iii–vii.
- Lee, A. (2002) "*A Scientific Methodology for MIS Case Studies*", IN: Myers, M. and Avison, D. (Eds.) "*Qualitative Research in Information Systems: A Reader*", London: Sage, pp.1–26.
- Lee, A. (2005) "*Thinking About Social Theory and Philosophy for Information Systems*", IN: Mingers, J. and Willcocks, L. (Eds.) "*Social Theory and Philosophy for Information Systems*", Chichester: John Wiley and Sons.
- Leuprecht, C., Skillicorn, D. and Tait, V. (2016) "*Beyond the Castle Model of Cyber-Risk and Cyber-Security*", *Government Information Quarterly*, Vol. 33, pp.250–257.
- Levay, C. and Waks, C. (2009) "*Professions and the Pursuit of Transparency in Healthcare: Two Cases of Soft Autonomy*", *Organization Studies*, Vol. 30, pp.509–527.
- Liljegren, A. (2012) "*Key Metaphors in the Sociology of Professions: Occupations as Hierarchies and Landscapes*", *Comparative Sociology*, No. 11, pp.88–112.
- Lindup, K. (1995) "*A New Model for Information Security Policies*", *Computers and Security*, Vol. 14, No. 8, pp.691–695.
- Loch, K., Carr, H. and Warkentin, M. (1992) "*Threats to Information Systems: Today's Reality, Yesterday's Understanding*", *Management Information Systems Quarterly*, Vol. 16, No. 2, pp. 173–186.
- Lui, S., Ngo, H. and Wing-Ngar Tsang, A. (2001) "*Interrole Conflict as a Predictor of Job Satisfaction and Propensity to Leave: A Study of Professional Accountants*", *Journal of Managerial Psychology*, Vol. 16, No. 6, pp.469–484.
- Lunt, I. (2008) "*Ethical Issues in Professional Life*", IN: Cunningham, B. (Ed.), "*Exploring Professionalism*", London: Institute of Education, University of London, pp.73–98.
- Macdonald, K. (1995) "*The Sociology of the Professions*", London: Sage.
- Mackenzie, D. and Pottinger, G. (1997) "*Mathematics, Technology, and Trust: Formal Verification, Computer Security, and the US Military*", *IEEE Annals of the History of Computing*, Vol. 19, No. 3, pp.41–59.
- Mahdavi, M. and Elliot, C. (2005) "*Integrating Security*", IN: Green, E. (Ed.) "*The Black Book on Corporate Security*", 2nd Edition, Potomac: Larstan Publishing, pp.101–128.

- Mangan, D. (2014) *"The Curiosity of Professional Status"*, Tottels Journal of Professional Negligence, Vol. 30, No. 2, pp.74–89.
- Mann, J. (2002) *"IT Education's Failure to Deliver Successful Information Systems: Now is the Time to Address the IT-User Gap"*, Journal of Information Technology Education, Vol. 1, No. 4, pp.252–267.
- Mansfield-Devine, S. (2013) *"Ian Glover, CREST – A Professional Approach to Information Assurance"*, Computer Fraud and Security, October 2013, pp.16–20.
- Manunta, G. (1999) *"What Is Security?"*, Security Journal, Vol. 12, No.3, pp.57–66.
- McBride, G. (2005) *"Overall Risk Management Strategy"*, IN: Green, E. (Ed.) *"The Black Book on Corporate Security"*, 2nd Edition, Potomac: Larstan Publishing.
- McFadzean, E., Ezingear, J.-N. and Birchall, D. (2006) *"Anchoring Information Security Governance Research: Sociological Groundings and Future Directions"*, Journal of Information System Security, Vol. 2, No. 3, pp.3–48.
- McFadzean, E., Ezingear, J.-N. and Birchall, D. (2007) *"Perception of Risk and the Strategic Impact of Existing IT on Information Security Strategy At Board Level"*, Online Information Review, Vol. 31, No. 5, pp.622–660.
- McGee, A. (2006) *"Corporate Security's Professional Project: An Examination of the Modern Condition of Corporate Security Management and the Potential for Further Professionalisation of the Occupation"*, Unpublished M.Sc. thesis, Cranfield University.
- McLean, C. and Hassard, J. (2004) *"Symmetrical Absence/Symmetrical Absurdity: Critical Notes on the Production of Actor–Network Accounts"*, Journal of Management Studies, Vol. 41, No. 3, pp.493–519.
- Miller, L. and Gregory, P. (2007) *"CISSP for Dummies"*, 2nd Edition, Hoboken: Wiley.
- Millerson, G. (1964) *"The Qualifying Associations: A Study in Professionalization"*, Abingdon: Routledge.
- Mok, H. (2010) *"A Review of the Professionalization of the Software Industry: Has it Made Software Engineering a Real Profession?"*, International Journal of Information Technology, Vol. 16, No.1, pp.61–75.
- Moritz, R. (2005) *"Blending Corporate Governance with Information Security"*, IN: Green, E. (Ed.) *"The Black Book on Corporate Security"*, 2nd Edition, Potomac: Larstan Publishing.
- Morris, R. and Thompson, K. (1979) *"Password Security: A Case History"*, Communications of the ACM, Vol. 22, No. 11, pp.594–597.
- Muzio, D., Brock, D. and Suddaby, R. (2013) *"Professions and Institutional Change: Towards an Institutional Sociology of the Professions"*, Journal of Management Studies, Vol. 50, No. 5, pp.699–721.
- Myers, M. (2004) *"Hermeneutics in Information Systems"*, IN: Mingers, J. and Willcocks, L. (Eds.) *"Social Theory and Philosophy for Information Systems"*, Chichester: John Wiley and Sons.
- Myers, M. (2011) *"Is There a Methodological Crisis?"*, Journal of Information Technology, Vol. 26,

pp.294–295.

Myers, M. and Avison, D. (2002) *"An Introduction to Qualitative Research in Information Systems"*, IN: Myers, M. and Avison, D. (Eds.) *"Qualitative Research in Information Systems: A Reader"*, London: Sage, pp.3–12.

Myers, M. and Klein, H. (2011) *"A Set of Principles for Conducting Critical Research in Information Systems"*, Management Information Systems Quarterly, Vol. 35, No. 1, pp.17–36.

Myers, M. and Newman, M. (2007) *"The Qualitative Interview in IS Research: Examining the Craft"*, Information and Organization, Vol. 17, pp.2–26.

National Computer Security Center [NCSC] (1992) *"A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems"* [online], Available at: <<http://www.fas.org/irp/nsa/rainbow/tg027.htm>> [Accessed 13/08/2011].

National Initiative for Cybersecurity Careers and Studies [NICCS] (2012a) *"A Historical Review of How Occupations Become Professions"* [online], Available at: <https://niccs.uscert.gov/sites/default/files/publications/documents/A_Historical_Review_of_How_Occupations_Become_Professions.pdf> [Accessed 26/08/2016].

National Initiative for Cybersecurity Careers and Studies [NICCS] (2012b) *"Best Practices for Implementing Professionalization"* [online], Available at: <https://niccs.uscert.gov/sites/default/files/publications/documents/Best_Practices_for_Implementing_Professionalization.pdf> [Accessed 26/08/2016].

National Research Council [NRC] (2013) *"Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-Making"*, Washington, DC: National Academies Press.

National Security Telecommunications and Information Systems Security [NSTISS] (1994) *"National Training Standard for Information Systems Security (Infosec) Professionals, NSTISSI No. 4011"* [online], Available at: <http://www.cnss.gov/assets/pdf/nstissi_4011.pdf> [Accessed 28/05/2011].

Neal, M. and Morgan, J. (2000) *"The Professionalization of Everyone? A Comparative Study of the Development of the Professions in the United Kingdom and Germany"*, European Sociological Review, Vol. 16, No. 1, pp.9–26.

Neal, R. (2008) *"Service-Oriented Security Architecture and its Implications for Security Department Organization Structures"*, Information Security Journal, Vol. 17, No. 4, pp.188–200.

Neumann, P. (2004) *"Computer Security and Human Values"*, IN: Bynum, T. and Rogerson, S. (Eds.) *"Computer Ethics and Professional Responsibility"*, Oxford: Blackwell, pp.208–226.

Ng, B.-Y., Kankanhalli, A. and Xu, Y. (2009) *"Studying Users' Computer Security Behavior: A Health Belief Perspective"*, Decision Support Systems, Vol. 46, pp.815–825.

Noordegraaf, M. (2007) *"From Pure to Hybrid Professionalism: Present Day Professionalism in Ambiguous Public Domains"*, Administration and Society, Vol. 39, No. 6, pp.761–785.

Office for National Statistics [ONS] (2007) *"UK Standard Industrial Classification 2007 (UK SIC 2007)"*,

Basingstoke: Macmillan.

Okenyi, P. and Owens, T. (2007) "*On the Anatomy of Human Hacking*", Information Systems Security, Vol. 16, No. 6, pp.302–314.

Olesen, K. and Myers, M. (1999) "*Trying to Improve Communication and Collaboration with Information Technology: An Action Research Project Which Failed*", Information Technology and People, Vol. 12, No. 4, pp.317–332.

Olmsted, A. and Paget, M. (1969) "*Some Theoretical Issues in Professional Socialization*", Academic Medicine, Vol. 44, No. 8, pp.663–669.

Oppliger, R. (2015) "*Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale*", IEEE Security and Privacy, Vol. 13, No. 6, pp.18–21.

Orlikowski, W. (1992) "*The Duality of Technology: Rethinking the Concept of Technology in Organizations*", Organization Science, Vol. 3, No. 3, pp.398–427.

Orlikowski, W. (1993) "*CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development*", Management Information Systems Quarterly, Vol. 17, No. 3, pp.309–340.

Orlikowski, W. and Baroudi, J. (1988) "*The Information Systems Profession: Myth or Reality?*", Office Technology and People, Vol. 4, No. 1, pp.13–30.

Orlikowski, W. and Baroudi, J. (2002) "*Studying Information Technology in Organizations: Research Approaches and Assumptions*", Information Systems Research, Vol. 2, No. 1, pp.1–28.

Orlikowski, W. and Robey, D. (1991) "*Information Technology and the Structuring of Organizations*", Information Systems Research, Vol. 2, No. 2, pp.143–169.

Oz, E. (1992) "*Ethical Standards for Information Systems Professionals: A Case for a Unified Code*", Management Information Systems Quarterly, Vol. 16, No. 4, pp.423–433.

Palmer, G. (2005) "*De-Perimeterisation: Benefits and Limitations*", Information Security Technical Report, Vol. 10, pp.189–203.

Parsons, T. (1939) "*The Professions and Social Structure*", Social Forces, Vol. 17, No. 4, pp.457–467.

Pemble, M. (2001) "*Licensed to... Well, to What? And, by Whom?*", Network Security, No. 10, pp.7–9.

Peneder, M. (2003) "*Industry Classifications: Aim, Scope and Techniques*", Journal of Industry, Competition and Trade, Vol. 3, No. 1, pp.109–129.

Post, G. and Kagan, A. (2007) "*Evaluating Information Security Tradeoffs: Restricting Access Can Interfere With User Tasks*", Computers and Security, Vol. 26, No. 3, pp.229–237.

Posthumus, S. and von Solms, R. (2004) "*A Framework for the Governance of Information Security*", Computers and Security, Vol. 23, No. 8, pp.638–646.

PriceWaterhouseCoopers (2011) "*2011 Global State of Information Security Survey*" [online], Accessible

at: <<http://www.pwc.com/gx/en/information-security-survey/pdf/giss-2011-survey-report.pdf>> [Accessed 03/09/2011].

Privy Council (2003) "*Royal Charter of the British Computer Society 1984, as Amended by Order in Council 13 November 2003*" [online], Available at: <<http://www.bcs.org/upload/pdf/royalcharter.pdf>> [Accessed 15/10/2012].

Puhakainen, P. and Siponen, M. (2010) "*Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study*", *Management Information Systems Quarterly*, Vol. 34, No. 4, pp.757–778.

Raffaelli, M. and Ontai, L. (2004) "*Gender Socialization in Latino/a Families: Results from Two Retrospective Studies*", *Sex Roles*, Vol. 50, No. 5/6, pp.287–299.

Rainer, R., Marshall, T., Knapp, K. and Montgomery, G. (2007) "*Do Information Security Professionals and Business Managers View Information Security Issues Differently?*", *Information Systems Security*, Vol. 16, No. 2, pp.100–108.

Raywood, D. (2012) "*Are CISOs About To Become About Much More Than Security?*" [online], Available at: <http://www.scmagazineuk.com/are-cisos-about-to-become-about-much-more-than-security/article/223626/?DCMP=EMC-SCUK_Newsire> [Accessed 30/01/2012].

Reader, W. (1966) "*Professional Men*", London: Weidenfeld and Nicolson.

Reece, R. and Stahl, B. (2015) "*The Professionalisation of Information Security: Perspectives of UK Practitioners*", *Computers and Security*, Vol. 48, pp.182–195.

Remenyi, D. (2012) "*Case Study Research*", Reading: Academic Publishing.

Renaud, K. (2012) "*Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches?*", *IEEE Security and Privacy*, Vol. 10, No. 3, pp.57–63.

Rhee, H., Ryub, Y. and Kim, C. (2012) "*Unrealistic Optimism on Information Security Management*", *Computers and Security*, Vol. 31, No. 2, pp.221–232.

Rhodes, J. (2009) "*Using Actor–Network Theory to Trace an ICT (Telecenter) Implementation Trajectory in an African Women's Micro-Enterprise Development Organization*", *Information Technologies and International Development*, Vol. 5, No. 3, pp.1–20.

Riege, A. (2003) "*Validity and Reliability tests in Case Study Research: A Literature Review with 'Hands-On' Applications for Each Research Phase*", *Qualitative Market Research*, Vol. 6, No. 2, pp.75–86.

Ritzer, G. (1973) "*Professionalism and the Individual*", IN: Freidson, E. (Ed.) "*The Professions and Their Prospects*", London: Sage, pp.59–74.

Rueschemeyer, D. (1983) "*Professional Autonomy and the Social Control of Expertise*", IN: Dingwall, R. and Lewis, P. (Eds.) "*The Sociology of the Professions: Lawyers, Doctors and Others*", London: Macmillan, pp.38–58.

Ruighaver, A., Maynard, S. and Chang, S. (2007) "*Organisational Security Culture: Extending the End-*

User Perspective", Computers and Security, Vol. 26, pp.56–62.

Ryan, J. and Jefferson, T. (2003) *"The Use, Misuse, and Abuse of Statistics in Information Security Research"*, Proceedings of the 2003 ASEM National Conference, St. Louis.

Ryan, J. and Ryan, D. (2006) *"Expected Benefits of Information Security Investments"*, Computers and Security, Vol. 25, No. 8, pp.579–588.

Safa, N., von Solms, R. and Furnell, S. (2016) *"Information Security Policy Compliance Model in Organizations"*, Computers and Security, Vol. 56, pp.70–82.

Saks, M. (1983) *"Removing the Blinkers? A Critique of Recent Contributions to the Sociology of Professions"*, The Sociological Review, Vol. 31, No. 1, pp.3–21.

Saks, M. (1995) *"Professions and the Public Interest"*, London: Routledge.

Saks, M. (2012) *"Defining a Profession: The Role of Knowledge and Expertise"*, Professionals and Professionalism, Vol. 2, No. 1, pp.1–10.

Saks, M. (2015) *"The Professions, State and the Market"*, New York: Routledge.

Saldaña, J. (2009) *"The Coding Manual for Qualitative Researchers"*, London: Sage.

Sandelowski, M., Voils, C. and Knafl, G. (2009) *"On Quantitizing"*, Journal of Mixed Methods Research, Vol. 3, No. 3, pp.208–222.

Sasse, A. (2015) *"Scaring and Bullying People into Security Won't Work"*, IEEE Security and Privacy, Vol. 13, No. 3, pp.80–83.

Sasse, A., Brostoff, S. and Weirich, D. (2001) *"Transforming the 'Weakest Link': A Human–Computer Interaction Approach for Usable and Effective Security"*, BT Technology Journal, Vol. 19, No. 3, pp.122–131.

Sayes, E. (2014) *"Actor–Network Theory and Methodology: Just What Does It Mean to Say That Nonhumans Have Agency?"*, Social Studies of Science, Vol. 44, No.1, pp.134–149.

Schneider, F. (2013) *"Cybersecurity Education in Universities"*, IEEE Security and Privacy, Vol. 11, No.4, pp.3–4.

Schneier, B. (2008) *"Schneier on Security"*, Indianapolis: Wiley.

Schreier, M. (2012) *"Qualitative Content Analysis in Practice"*, London: Sage.

Schultz, E. (2005) *"Infosec Certification: Which Way Do We Turn From Here?"*, Computers and Security, Vol. 24, pp.587–588.

Sciulli, D. (2007) *"Paris Visual Académie as First Prototype Profession: Rethinking the Sociology of Professions"*, Theory Culture Society Vol. 24, pp.35–59.

Scott-Smith, T. (2013) *"Actor - Network Theory for Development Working Paper Series Paper No. 3 The Least Provocative Path: An ANT Lens on Development Project Formation and Dissolution"* [online], Available at: <http://hummedia.manchester.ac.uk/institutes/cdi/resources/cdi_ant4d/ANT4DWorking

Seeholzer, R. (2012) *"Information Security Strategy: In Search of a Role"*, IN: *"Proceedings of the 2012 Americas Conference on Information Systems"*, Vol. 1, pp.144–161.

Sharma, S. and Sefchek, J. (2007) *"Teaching Information Systems Security Courses: A Hands-On Approach"*, Computers and Security, Vol. 26, pp.290–299.

Silic, M. and Back, A. (2014) *"Information Security: Critical Review and Future Directions for Research"*, Information Management and Computer Security, Vol. 22, No.3, pp.279–308.

Silverman, D. (2000) *"Doing Qualitative Research: A Practical Handbook"*, Thousand Oaks: Sage.

Siponen, M. (2000) *"A Conceptual Foundation for Organizational Information Security Awareness"*, Information Management and Computer Security, Vol. 8, No. 1, pp.31–41.

Siponen, M. (2001) *"An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications"*, IN: Dhillon, G. (Ed.) *"Information Security Management: Global Challenges in the New Millenium"*, Hershey: Idea Group, pp.101–124.

Siponen, M. (2005) *"Analysis of Modern IS Security Development Approaches: Towards the Next Generation of Social and Adaptable ISS Methods"*, Information and Organization, Vol. 15, pp.339–375.

Siponen, M. (2006) *"Information Security Standards Focus on the Existence of Process, Not Its Content"*, Communications of the ACM, Vol. 49, No. 8, pp.97–100.

Siponen, M. and Oinas-Kukkonen, H. (2007) *"A Review of Information Security Issues and Respective Research Contributions"*, SIGMIS Database for Advances in Information Systems, Vol. 38, No. 1, pp.60–80.

Siponen, M. and Vance, A. (2010) *"Neutralization: New Insights Into the Problem of Employee Information Systems Security Policy Violations"*, Management Information Systems Quarterly, Vol. 34, No. 3, pp.487–502.

Siponen, M. and Willison, R. (2009) *"Information Security Management Standards: Problems and Solutions"*, Information and Management, Vol. 46, pp.267–270.

Siponen, M., Mahmood, A. and Pahnla, S. (2014) *"Employees' Adherence to Information Security Policies: An Exploratory Field Study"*, Information and Management, Vol. 51, pp.217–224.

Siponen, M., Willison, R. and Baskerville, R. (2008) *"Power and Practice in Information Systems Security Research"*, Proceedings of ICIS 2008, Paper 26.

Son, J.-Y. (2011) *"Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies"*, Information Management, Vol. 48, No. 7, pp.296–302.

Soomro, Z., Shah, M. and Ahmed, J. (2016) *"Information Security Management Needs More Holistic Approach: A Literature Review"*, International Journal of Information Management, Vol. 36, pp.215–225.

Spagnoletti, P. and Resca, A. (2008) *"The Duality of Information Security Management: Fighting Against Predictable and Unpredictable Threats"*, Journal of Information Systems Security, Vol. 4, No. 3, pp.46–

- Spanos, G. and Angelis, L. (2016) *"The Impact of Information Security Events to the Stock Market: A Systematic Literature Review"*, Computers and Security, Vol. 58, pp.216–229.
- Stahl, B. (2006) *"Is Forensic Computing a Profession? Revisiting an Old Debate in a New Field"*, Journal of Digital Forensics, Security and Law, Vol. 1, No. 4, pp.49–66.
- Stahl, B. (2008) *"The Impact of the UK Human Rights Act 1998 on Privacy Protection in the Workplace"*, IN: Subramanian, R. (Ed.) *"Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solutions"*, Hershey: Idea Group, pp.55–68.
- Stahl, B. (2014) *"Interpretive Accounts and Fairy Tales: A Critical Polemic Against the Empiricist Bias in Interpretive IS Research"*, European Journal of Information Systems, Vol. 23, No. 1, pp.1–11.
- Stahl, B., Doherty, N. and Shaw, M. (2012) *"Information Security Policies in the UK Healthcare Sector: A Critical Evaluation"*, Information Systems Journal, Vol. 22, No. 1, pp.77–94.
- Stahl, B., Doherty, N., Shaw, M. and Janicke, H. (2014) *"Critical Theory as an Approach to the Ethics of Information Security"*, Science and Engineering Ethics, Vol. 20, No. 3, pp.675–699.
- Stahl, B., Shaw, M. and Doherty, N. (2008) *"Information Systems Security: A Critical Research Agenda"* IN: *"Association of Information Systems SIGSEC Workshop on Information Security and Privacy (WISP 2008)"*, December 13, 2008, Paris, France.
- Stanton, J., Stam, K., Mastrangelo, P. and Jolton, J. (2005) *"Analysis of End User Security Behaviours"*, Computer Security, Vol. 24, pp.124–133.
- Stewart, A. (2012) *"Can Spending on Information Security Ever Be Justified? Evaluating the Security Spending Decision from the Perspective of a Rational Actor"*, Information Management and Computer Security, Vol. 20, No. 4, pp.312–326.
- Stewart, G. and Lacey, D. (2012) *"Death by a Thousand Facts: Criticising the Technocratic Approach to Information Security Awareness"*, Information Management and Computer Security, Vol. 20, No. 1, pp.29–38.
- Stowell, F. and Mingers, J. (1997) *"Information Systems: An Emerging Discipline? – Introduction"*, IN: Stowell, F. and Mingers, J. (Eds.) *"Information Systems: An Emerging Discipline?"*, London: McGraw Hill.
- Straub, D. (1990) *"Effective IS Security: An Empirical Study"*, Information Systems Research, Vol. 1, No. 3, pp.255–276.
- Straub, D. and Welke, R. (1998) *"Coping With Systems Risk: Security Planning Models for Management Decision Making"*, Management Information Systems Quarterly, pp.441–469.
- Suddaby, R., Cooper, D. and Greenwood, R. (2007) *"Transnational Regulation of Professional Services: Governance Dynamics of Field Level Organizational Change"*, Accounting, Organizations and Society, Vol. 32, Nos. 4–5, pp.333–362.

- Suetonius Tranquillus, C. (121) *"The Twelve Caesars: Caus Julius Caesar"*, Translated by Alexander Thomson, Chios Classics.
- Sundt, C. (2006) *"Information Security and the Law"*, Information Security Technical Report, Vol. 11, No. 1, pp.2–9.
- Susskind, R. and Susskind, D. (2015) *"The Future of the Professions"*, Oxford: Oxford University Press.
- Swindle, O. and Conner, B. (2004) *"The Link Between Information Security and Corporate Governance"* [Online], Available at: <http://www.computerworld.com/s/article/92915/The_Link_Between_Information_Security_and_Corporate_Governance> [Accessed 23/09/2011].
- Talbot, J. (1981) *"Management Guide to Computer Security"*, Gower Publishing Ltd.
- Tankard, C. (2016) *"What the GDPR Means for Businesses"*, Network Security, No. 6, pp.5–8.
- Tate, N., Lichtenstein, S. and Warren, M. (2008) *"IT Security Certifications: Stakeholder Evaluation and Selection"*, IN: *"Proceedings of the 19th Australasian Conference on Information Systems"*, Christchurch, pp.991–1001.
- Tatnall, A. and Burgess, S. (2002) *"Using Actor–Network Theory to Research the Implementation of a BB Portal for Regional SMEs in Melbourne, Australia"*, Proceedings of the 15th Bled Electronic Commerce Conference, *"eReality: Constructing the eEconomy"*, Bled, Slovenia, University of Maribor.
- Tatnall, A. and Gilding, A. (1999) *"Actor–Network Theory and Information Systems Research"*, IN: *"Proceedings of the 10th Australasian Conference on Information Systems"*, pp.955–966.
- Tech Partnership (2016) *"IT Professional Standards (Information Security - New)"* [online], Accessible at: <<https://www.thetechpartnership.com/standards-and-quality/it-professional-standards/information-security>> [accessed 13/06/16].
- Thomas, D. (2006) *"A General Inductive Approach for Analyzing Qualitative Evaluation Data"*, American Journal of Evaluation, Vol. 27, No. 2, pp.237–246.
- Thomson, K. and van Niekerk, J. (2012) *"Combating Information Security Apathy by Encouraging Prosocial Organisational Behaviour"*, Information Management and Computer Security, Vol. 20, No. 1, pp.39–46.
- Thomson, K.-L. and von Solms, R. (2005) *"Information Security Obedience: A Definition"*, Computers and Security, Vol. 24, pp.69–75.
- Thomson, M. and von Solms, R. (1998) *"Information Security Awareness: Educating Your Users Effectively"*, Information Management and Computer Security, Vol. 6, No. 4, pp.167–173.
- Trompeter, C. and Eloff, J. (2001) *"A Framework for the Implementation of Socio-Ethical Controls in Information Security"*, Computers and Security, Vol. 20, No.5, pp.384–391.
- US Department of Defence [US DoD] (2010) *"DoD 8570.01-M Information Assurance Workforce Improvement Program"* [online], Available at: <<http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>> [Accessed 03/09/2011].

- US Department of Health and Human Services [US DoHHS] (2011) "*Summary of the HIPAA Security Rule*" [Online], Available at: <<http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html>> [Accessed 04/06/2011].
- US Department of Homeland Security [US DoHS] (2012) "*Homeland Security Advisory Council Cyberskills Task Force Report*" [online], Available at: <<http://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf>> [Accessed 12/10/2016].
- Van Biene-Hershey, M. (2007) "*IT Security and Auditing Between 1960 and 2000*", IN: De Leeuw, K. and Bergstra, J. (Eds.) "*The History of Information Security*", London: Elseiver, pp.655–680.
- Van de Kamp, K., Vernooij-Dassen, M., Grol, R. and Bottema, B. (2004) "*How to Conceptualize Professionalism: A Qualitative Study*", Medical Teacher, Vol. 26, No. 8, pp.696–702.
- Van Niekerk, J. and von Solms, R. (2010) "*Information Security Culture: A Management Perspective*", Computers and Security, Vol. 29, pp.476–486.
- Van Tassel, D. (1972) "*Computer Security Management*", Hemel Hempstead: Prentice Hall.
- Vance, A., Siponen, M. and Pahlila, S. (2012) "*Motivating IS Security Compliance: Insights From Habit and Protection Motivation Theory*", Information and Management, Vol. 49, No. 3, pp.190–198.
- Von Solms, R. (1999) "*Information Security Management: Why Standards are Important*", Information Management and Computer Security, Vol. 7, No. 1, pp.50–58.
- Von Solms, R. and van Niekerk, J. (2013) "*From Information Security to Cyber Security*", Computers and Security, Vol. 38, pp.97–102.
- Von Solms, S. (2000) "*Information Security – The Third Wave?*", Computers and Security, Vol. 19, pp.615–620.
- Von Solms, S. (2001a) "*Information Security – A Multidimensional Discipline*", Computers and Security, Vol. 20, pp.504–508.
- Von Solms, S. (2001b) "*Corporate Governance and Information Security*", Computers and Security, Vol. 20, pp.215–218.
- Von Solms, S. (2006) "*Information Security – The Fourth Wave*", Computers and Security, Vol. 25, pp. 165–168.
- Von Solms, S. and von Solms, R. (2004) "*The 10 Deadly Sins of Information Security Management*", Computers and Security, Vol. 23, No. 5, pp.371–376.
- Von Solms, S. and von Solms, R. (2008) "*Information Security Governance*", London: Springer Science.
- Vroom, C. and von Solms, R. (2004) "*Towards Information Security Behavioural Compliance*", Computers and Security, Vol. 23, pp.191–198.
- Walsham, G. (1995) "*The Emergence of Interpretivism in IS Research*", Information Systems Research, Vol. 6, No. 4, pp.376–394.

- Walsham, G. (1997) *"Actor–Network Theory and IS Research: Current Status and Future Prospects"*, IN: Lee, A., Liebenau, J. and DeGross, J. (Eds.) *"Information Systems and Qualitative Research"*, London: Chapman and Hall.
- Walton, R. (2006) *"The Computer Misuse Act"*, Information Security Technical Report, Vol. 11, pp.39–45.
- Wang, T. (1988) *"Some Problems Arising out of the Cross-Disciplinary Nature of Information Systems Security"*, Proceedings of the 21st Annual Hawaii International Conference on System Sciences, Vol. 4, IEEE, pp.208–217.
- Wang, Y., Yuan, Y., Turel, O. and Tu, Z. (2015) *"Understanding the Development and Diffusion of Mobile Commerce Technologies in China: A Biographical Study with an Actor–Network Theory Perspective"*, International Journal of Electronic Commerce, Vol. 19, No. 4, pp.47–76.
- Ware, W. (1970) *"Security Controls for Computer Systems"* [online], Available at: <<http://csrc.nist.gov/publications/history/ware70.pdf>> [Accessed 10/06/2011].
- Watt, S. (1989) *"Computer Security Manager"*, Elsevier Science.
- Werlinger, R., Hawkey, K. and Beznosov, K. (2009) *"An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management"*, Information Management and Computer Security, Vol. 17, No. 1, pp.4–19.
- White, G., Conklin, A., Cothren, C., Davis, R. and Williams, D. (2003) *"Security + Certification All-in-One Exam Guide"*, Emeryville: McGraw-Hill.
- Whitman, M. (2003) *"Enemy at the Gate: Threats to Information Security"*, Communications of the ACM, Vol. 46, No. 8, pp.91–95.
- Whitman, M. and Mattord, H. (2009) *"Principles of Information Security"*, London: Cengage Learning.
- Whittle, A and Spicer, A. (2008) *"Is Actor Network Theory Critique?"*, Organization Studies, Vol. 29, pp.611–629.
- Wilensky, H. (1964) *"The Professionalization of Everyone?"*, American Journal of Sociology, Vol. 70, No. 2, pp.137–158.
- Williams, M. (2000) *"Interpretivism and Generalisation"*, Sociology, Vol. 34, No. 2, pp.209–224.
- Willison, R. and Siponen, M. (2007) *"A Critical Assessment of IS Security Research Between 1990–2004"*, IN: Proceedings of 15th European Conference on ISs, St. Gallen, Switzerland, pp.1551–1559.
- Winder, D. (2009) *"Anatomy of a CISO"*, InfoSecurity Magazine, November/December 2009.
- Winner, L. (1993) *"Upon Opening the Black Box and Finding it Empty: Social Constructivism and the Philosophy of Technology"*, Science Technology and Human Values, Vol. 18, No. 3, pp.362–378.
- Wooldridge, S., Corder, C. and Johnson, C. (1973) *"Security Standards for Data Processing"*, London: Macmillan Press.
- Wright, M. (1998) *"The Need for Information Security Education"*, Computer Fraud and Security, No. 8,

pp.14–17.

Yost, J. (2015) "*The Origin and Early History of the Computer Security Software Products Industry*", IEEE Annals of the History of Computing, Vol. 37, No. 2, pp.46–58.

Appendix 1: Interview Instruments

The instruments as actually used are recreated in the following order. Due to differences between margin and footer sizes between documents there may be trivial differences in layout from copies physically used.

Section 1: Notes for Participants

- Academic (Course leaders in UK Universities)
- Professional Bodies (Senior managers of certifying institutions)
- Government (UK central government)
- Practitioners (People with IS responsibility organisations in various sectors)

Section 2: Interview Protocol

- Academic (v.1)
- Professional Bodies (v. 1)
- Government (v. 1.02 as used)
- Practitioners (v. 1.02 Original, for Pilot)
- Practitioners (v. 1.1 Updated for Main Phase, see Section 4.7.3)

Interviewee Explanatory Notes and Consent Form [1 of 4]

(Academic Participants)

Thank you for considering participating in this research. Please take a moment to read through the information below which explains what is being requested, your rights to withdraw and how your information will be processed and stored.

What is the purpose of the research?

The purpose is to investigate issues of *professional status* amongst those who manage information security in commercial, public, charitable and other organisations. It aims to examine these issues from the perspective of those who perform the role themselves, those whose work might affect the professional status of the occupation (for example national associations, universities and qualifications bodies) and those in government who are in a position to regulate it. Please feel free to discuss the aims of the project in greater detail before deciding whether to participate. Your information will be used only for the stated academic purposes.

What is the format of the research?

Your contribution will take the form of a *semi-structured interview*. In this format the interviewer has a list of topics to help guide the conversation, however the participants are free to follow any points of interest, or examples which the interviewee considers particularly relevant, as they arise. If English is not your first language and you would like any adjustment such as slower speech or being accompanied by a translator, please do feel free to request this.

Why do you want an audio recording of the interview?

As is common practice with such interviews, with your permission the interview will be recorded. This is because the particular method of analysis which will be used requires the interview to be first transcribed verbatim. This is considerably more efficient if performed later from a recording as it allows the conversation to flow naturally, and is more interesting for the participants. You will be sent a copy of the transcript so that you can correct any errors of transcription if you choose. This is also an opportunity to identify any data you would prefer not to be used in the analysis (see below) for whatever reason. As the location for the interview is often at the interviewee's place of work, please bring to the interviewer's attention any possibility that private, personal, confidential or commercially sensitive information might be inadvertently captured by the recording device from surrounding areas.

Who is the interviewer?

The interviewer is a part-time postgraduate student studying for a research degree with the Centre for Computing and Social Responsibility at De Montfort University in Leicester, UK and is bound by that institution's ethical and disciplinary codes. The interviewer is also a network engineer employed in the aerospace industry however he is acting entirely in the capacity of student and *not in any way* in his capacity as an employee of any other organisation. Although this is unlikely, if you are aware of any potential conflict of interest which may arise from your participation please bring this to the attention of the interviewer.

Will you ask me about my organisation's IT security or other confidential information?

No, this is not the purpose of the study; the intention of the research is to understand the professional status of information security practitioners from the perspective of the interviewee and does not concern the security policy or practice of their employer. The topics covered will be: your career background and how you came to work in the field, the importance of security as a topic and the events which have affected this, the origins of your organisation's security-related degree programmes and their content and syllabus, student demographics, perceived motivations and attitudes, comparison of academic and industry qualifications, and the professionalisation of the industry and its relative status.

Should you wish to decline to answer any question to avoid revealing sensitive or confidential information, or for any other reason, you are entirely free to do so. Should you happen to use specific information from your current or a former organisation (or student thereof) to illustrate a point it will be treated as confidential or made anonymous as described below, and you are free to request that whilst doing so the recording is paused and/or that the information not be used in the analysis. You are also able to request withdrawal of that information later as described below.

Can I withdraw?

Participation is entirely voluntary and your consent may be withdrawn at any time during or after the interview. Should you withdraw before the end of the interview or later but before any analysis has begun, all recordings and transcripts of the interview will be destroyed and this will be confirmed back to you when complete. No further use of any information provided by you will be made. Alternatively you may indicate that certain passages or responses should be removed, in which case these will not be transcribed (or removed from the transcription as appropriate) and these sections will not be used in the analysis.

Should you withdraw after the interview has been transcribed and analysis has begun, information from your interview may have already been combined with that of other participants to form theories and conclusions. In this eventuality, the recordings and transcripts of your own contribution will be destroyed and take no further part in the analysis, however it may not be practical to remove those theories and conclusions which were based in part on your information. In these circumstances, all reasonable efforts will be made to remove data from your interview from the analysis.

How will you handle my data? Will my contribution be confidential?

Recordings will be transcribed as soon as possible after the interview and thereafter stored in an encrypted format. The original recording file will be stored offline on optical media in a secure location for backup purposes. Once the interview has been transcribed and the accuracy of the transcription confirmed by the interviewee, the recording will not be accessed again unless the examiners wish to check the quality of the transcription process or for another official university purpose. All materials other than the submitted dissertation (and published papers or interim results, if any) will be stored and eventually destroyed according to the provisions of the De Montfort University research records retention policy, which is available at <http://www.dmu.ac.uk/documents/about-dmu-documents/quality-management-and-policy/records-management/research-records-retention-policy.pdf>

Each person participating will be assigned an anonymising code which is used to identify their data during analysis and in the dissertation. This code contains a serial number and an indication of job role. Thus, once the data has been transcribed it will no longer be personally identifiable by anyone other than the student and his supervisory/examination team. Likewise, the name of your organisation will be removed from the transcript and replaced with an identification code during analysis which specifies only its approximate size and industry sector. Any excerpts quoted will be edited to ensure that the identity of the speaker cannot be deduced from the context. Any reference to specific institutions, brands or individuals will similarly be made non-identifiable unless this is clearly unnecessary. The version sent to you as a transcript (after any changes requested have been made) will be the version used in the analysis therefore you will be able to request any further removal of information necessary.

Why use codes- why not remove all identifying data?

Firstly so that you can be sent your own transcript for verification. Secondly, it may be necessary to identify and remove the contribution of someone who later withdraws from the study.

What will my contribution be used for?

Information – once transcribed, anonymised and analysed – may be presented in the student's dissertation, internal progress reports, academic or industrial journal or magazine articles, conference posters or presentations to support an argument or conclusion, or to demonstrate examples of opinions observed. This may take the form of verbatim quotes or as summarised, interpreted or paraphrased text, numbers, tables or other formats. This information may be attributed to the source, if so this will be by serial number, pseudonym or terms of the information listed above (job role, and employer size and industry sector) and never the identity of the participant.

Consent

I agree to participate in the research for the purposes described above. I understand that my participation is voluntary and that I can withdraw at any time and without giving a reason. I am eighteen years of age or older.

Signed _____ Date _____

Name _____

Interviewee Explanatory Notes and Consent Form [2 of 4]

(Credential/Professional Body Participants)

Thank you for considering participating in this research. Please take a moment to read through the information below which explains what is being requested, your rights to withdraw and how your information will be processed and stored.

What is the purpose of the research?

The purpose is to investigate issues of *professional status* amongst those who manage information security in commercial, public, charitable and other organisations. It aims to examine these issues from the perspective of those who perform the role themselves, those whose work might affect the professional status of the occupation (for example national associations, universities and qualifications bodies) and those in government who are in a position to regulate it. Please feel free to discuss the aims of the project in greater detail before deciding whether to participate. Your information will be used only for the stated academic purposes.

What is the format of the research?

Your contribution will take the form of a *semi-structured interview*. In this format the interviewer has a list of topics to help guide the conversation, however the participants are free to follow any points of interest, or examples which the interviewee considers particularly relevant, as they arise. If English is not your first language and you would like any adjustment such as slower speech or being accompanied by a translator, please do feel free to request this.

Why do you want an audio recording of the interview?

As is common practice with such interviews, with your permission the interview will be recorded. This is because the particular method of analysis which will be used requires the interview to be first transcribed verbatim. This is considerably more efficient if performed later from a recording as it allows the conversation to flow naturally, and is more interesting for the participants. You will be sent a copy of the transcript so that you can correct any errors of transcription if you choose. This is also an opportunity to identify any data you would prefer not to be used in the analysis (see below) for whatever reason. As the location for the interview is often at the interviewee's place of work, please bring to the interviewer's attention any possibility that private, personal, confidential or commercially sensitive information might be inadvertently captured by the recording device from surrounding areas.

Who is the interviewer?

The interviewer is a part-time postgraduate student studying for a research degree with the Centre for Computing and Social Responsibility at De Montfort University in Leicester, UK and is bound by that institution's ethical and disciplinary codes. The interviewer is also a network engineer employed in the aerospace industry however he is acting entirely in the capacity of student and *not in any way* in his capacity as an employee of any other organisation. Although this is unlikely, if you are aware of any potential conflict of interest which may arise from your participation please bring this to the attention of the interviewer.

Will you ask me about my organisation's IT security or other confidential information?

No, this is not the purpose of the study; the intention of the research is to understand the professional status of information security practitioners from the perspective of the interviewee and does not concern the security policy or practice of their employer. The topics covered will be: your career background and how you came to work in the field, the importance of security as a topic and the events which have affected this, the reasons for the foundation of your organisation, the nature of information security practice, the role of credential-issuing bodies, comparison of academic and industry qualifications, the nature of professional status, the professionalisation of the industry and its relative status and maturity.

Should you wish to decline to answer any question to avoid revealing sensitive or confidential information, or for any other reason, you are entirely free to do so. Should you happen to use specific information from your current or a former organisation to illustrate a point it will be treated as confidential or made anonymous as described below, and you are free to request that whilst doing so the recording is paused and/or that the information not be used in the analysis. You are also able to request withdrawal of that information later as described below.

Can I withdraw?

Participation is entirely voluntary and your consent may be withdrawn at any time during or after the interview. Should you withdraw before the end of the interview or later but before any analysis has begun, all recordings and transcripts of the interview will be destroyed and this will be confirmed back to you when complete. No further use of any

information provided by you will be made. Alternatively you may indicate that certain passages or responses should be removed, in which case these will not be transcribed (or removed from the transcription as appropriate) and these sections will not be used in the analysis.

Should you withdraw after the interview has been transcribed and analysis has begun, information from your interview may have already been combined with that of other participants to form theories and conclusions. In this eventuality, the recordings and transcripts of your own contribution will be destroyed and take no further part in the analysis, however it may not be practical to remove those theories and conclusions which were based in part on your information. In these circumstances, all reasonable efforts will be made to remove data from your interview from the analysis.

How will you handle my data? Will my contribution be confidential?

Recordings will be transcribed as soon as possible after the interview and thereafter stored in an encrypted format. The original recording file will be stored offline on optical media in a secure location for backup purposes. Once the interview has been transcribed and the accuracy of the transcription confirmed by the interviewee, the recording will not be accessed again unless the examiners wish to check the quality of the transcription process or for another official university purpose. All materials other than the submitted dissertation (and published papers or interim results, if any) will be stored and eventually destroyed according to the provisions of the De Montfort University research records retention policy, which is available at <http://www.dmu.ac.uk/documents/about-dmu-documents/quality-management-and-policy/records-management/research-records-retention-policy.pdf>

Each person participating will be assigned an anonymising code which is used to identify their data during analysis and in the dissertation. This code contains a serial number and an indication of job role. Thus, once the data has been transcribed it will no longer be personally identifiable by anyone other than the student and his supervisory/examination team. Likewise, the name of your organisation will be removed from the transcript and replaced with an identification code during analysis which specifies only its approximate size and industry sector. Any excerpts quoted will be edited to ensure that the identity of the speaker cannot be deduced from the context. Any reference to specific institutions, brands or individuals will similarly be made non-identifiable unless this is clearly unnecessary. The version sent to you as a transcript (after any changes requested have been made) will be the version used in the analysis therefore you will be able to request any further removal of information necessary.

Why use codes- why not remove all identifying data?

Firstly so that you can be sent your own transcript for verification. Secondly, it may be necessary to identify and remove the contribution of someone who later withdraws from the study.

What will my contribution be used for?

Information – once transcribed, anonymised and analysed – may be presented in the student's dissertation, internal progress reports, academic or industrial journal or magazine articles, conference posters or presentations to support an argument or conclusion, or to demonstrate examples of opinions observed. This may take the form of verbatim quotes or as summarised, interpreted or paraphrased text, numbers, tables or other formats. This information may be attributed to the source, if so this will be by serial number, pseudonym or terms of the information listed above (job role, and employer size and industry sector) and never the identity of the participant.

Consent

I agree to participate in the research for the purposes described above. I understand that my participation is voluntary and that I can withdraw at any time and without giving a reason. I am eighteen years of age or older.

Signed _____ Date _____

Name _____

Interviewee Explanatory Notes and Consent Form (Government Participants) [3 of 4]

Thank you for considering participating in this research. Please take a moment to read through the information below which explains what is being requested, your rights to withdraw and how your information will be processed and stored.

What is the purpose of the research?

The purpose is to investigate issues of *professional status* amongst those who manage information security in commercial, public, charitable and other organisations. It aims to examine these issues from the perspective of those who perform the role themselves, those whose work might affect the professional status of the occupation (for example national associations, universities and qualifications bodies) and those in Government who are in a position to regulate it. Please feel free to discuss the aims of the project in greater detail before deciding whether to participate. Your information will be used only for the stated academic purposes.

What is the format of the research?

Your contribution will take the form of a *semi-structured interview*. In this format the interviewer has a list of topics to help guide the conversation, however the participants are free to follow any points of interest, or examples which the interviewee considers particularly relevant, as they arise. If English is not your first language and you would like any adjustment such as slower speech or being accompanied by a translator, please do feel free to request this.

Why do you want an audio recording of the interview?

As is common practice with such interviews, with your permission the interview will be recorded. This is because the particular method of analysis which will be used requires the interview to be first transcribed verbatim. This is considerably more efficient if performed later from a recording as it allows the conversation to flow naturally, and is more interesting for the participants. You will be sent a copy of the transcript for approval so that you can correct any errors of transcription if you choose. This is also an opportunity to identify any data you would prefer not to be used in the analysis (see below) for whatever reason.

Your particular attention is drawn to the following:

As the location for the interview could include secure facilities, please bring to the interviewer's attention any possibility that private, personal, confidential, protectively marked or otherwise sensitive information might be inadvertently captured by the recording device from surrounding areas. It would be very much appreciated if you could arrange for a private area such as a meeting room or office to be available for the interview if possible. It is assumed that all information discussed will be deemed public unless explicitly notified otherwise, i.e. is not subject to embargo, is not protectively marked and attracts no handling descriptor, national caveat or similar restriction. Other than for embargoed information, please request that the recording is stopped prior to revealing any information for which this is not the case.

Who is the interviewer?

The interviewer is a British part-time postgraduate student studying for a research degree with the Centre for Computing and Social Responsibility at De Montfort University in Leicester, UK and is bound by that institution's ethical and disciplinary codes. The interviewer is also employed as a network engineer and manager in a European aerospace and defence company, whose customers include the UK and other national governments, however he is acting entirely in the capacity of student and *not in any way* in his capacity as an employee of that organisation. If you are aware of any potential conflict of interest which may arise from your participation please bring this to the attention of the interviewer.

What are the topics for the interview?

The intention of the research is to investigate the current status and future prospects for the professionalisation of information security. The purpose of this interview is to gather the perspective of those responsible for UK Government policy in this area. The guide topics covered will be: interviewee career path (how they came to be in their role and whether they trained in information security), the origin of their role, the nature of modern information security practice, current availability of skilled staff, present and future security career paths, CCP scheme (reason for creation), the role of security certifications, the role and control of academic qualifications, the nature of professional status, the status of the information security industry, and the role of government in the regulation of information security.

Should you wish to decline to answer any question to avoid revealing sensitive or confidential information, or for any other reason, you are entirely free to do so. Should you happen to use specific information from your current or a former role to illustrate a point it will be treated as confidential or made anonymous where possible as described below, and you are free to request that whilst doing so the recording is paused and/or that the information not be used in the analysis. You are also able to request withdrawal of that information later as described below. *(continues overleaf)*

Can I withdraw?

Participation is entirely voluntary and your consent may be withdrawn at any time during or after the interview. Should you withdraw before the end of the interview or later but before any analysis has begun, all recordings and transcripts of the interview will be destroyed and this will be confirmed back to you when complete. No further use of any information provided by you will be made. Alternatively you may indicate that certain passages or responses should be removed, in which case these will not be transcribed (or removed from the transcription as appropriate) and these sections will not be used in the analysis.

Should you withdraw after the interview has been transcribed and analysis has begun, information from your interview may have already been combined with that of other participants to form theories and conclusions. In this eventuality, the recordings and transcripts of your own contribution will be destroyed and take no further part in the analysis, however it may not be practical to remove those theories and conclusions which were based in part on your information. In these circumstances, all reasonable efforts will be made to remove data from your interview from the analysis.

How will you handle my data? Will my contribution be confidential?

Recordings will be transcribed as soon as possible after the interview and thereafter stored in an encrypted format. The original recording file will be stored offline on optical media in a secure location for backup purposes. Once the interview has been transcribed and the accuracy of the transcription confirmed by the interviewee, the recording will not be accessed again unless the examiners wish to check the quality of the transcription process or for another official university purpose. All materials other than the submitted dissertation (and published papers or interim results, if any) will be stored and eventually destroyed according to the provisions of the De Montfort University research records retention policy, which is available at <http://www.dmu.ac.uk/documents/about-dmu-documents/quality-management-and-policy/records-management/research-records-retention-policy.pdf>

Please bear in mind that whilst the name of the individual(s) participating and the agency or department for which they work will not be revealed outside the above provisions, interviewees will be identified as influential staff in the agency responsible for the regulation and professionalisation of IT security in the UK. **It is therefore very likely that the identity of the agency and the interviewee could still be deduced by knowledgeable readers.** The text of the transcript may be explicitly presented by the student as – and/or inferred by the reader to be – the official and public position of the UK Government as of the date of the interview, unless stated otherwise.

During transcription, wherever possible and appropriate any references to specific institutions, brands or individuals will be made non-identifiable unless this is clearly unnecessary. The version sent to you as a transcript (after any changes requested have been made) will be the version used in the analysis therefore you will be able to request any further removal of information necessary.

Why use codes- why not remove all identifying data?

Firstly so that you can be sent your own transcript for verification. Secondly, it may be necessary to identify and remove the contribution of someone who later withdraws from the study.

What will my contribution be used for?

Information – once transcribed, anonymised and analysed – may be presented in the student's dissertation, internal progress reports, academic or industrial journal or magazine articles, conference posters or presentations to support an argument or conclusion, or to demonstrate examples of opinions observed. This may take the form of verbatim quotes or as summarised, interpreted or paraphrased text, numbers, tables or other formats. This information may be attributed to the source, if so this will be by serial number, pseudonym or terms of the information listed above (job role, and employer size and industry sector) and never the personal identity of the participant.

Consent

I agree to participate in the research for the purposes described above. I understand that my participation is voluntary and that I can withdraw at any time and without giving a reason. I am eighteen years of age or older.

Signed _____ Date _____

Name _____

Interviewee Explanatory Notes and Consent Form [Practitioners, 4 of 4]

Thank you for considering participating in this research. Please take a moment to read through the information below which explains what is being requested, your rights to withdraw and how your information will be processed and stored.

What is the purpose of the research?

The purpose is to investigate issues of the *professional status* of those who manage IT security in commercial, public and other organisations. It aims to examine these issues from the perspective of those who perform the role themselves, those who aim to advance the status of the profession (for example national associations and qualifications bodies) and those in government. Please feel free to discuss the aims of the project in greater detail before deciding whether to participate. Your information will be used only for the stated academic purposes.

What is the format of the research?

Your contribution will take the form of a *semi-structured interview*. In this format the interviewer has a list of topics to help guide the conversation, however the participants are free to follow any points of interest, or examples which the interviewee considers particularly relevant, as they arise. If English is not your first language and you would like any adjustment such as slower speech or being accompanied by a translator please do feel free to request this.

As is common with such interviews, with your permission the interview will be recorded. This is because the particular method of analysis which will be used requires the interview to be first transcribed verbatim. This is considerably more efficient if performed later from a recording as it allows the conversation to flow naturally and is more interesting for the participants. You will be sent a copy of the transcript so that you can correct any errors of transcription. This is also an opportunity to identify any data you would prefer not to be used in the analysis (see below) for whatever reason.

Who is the interviewer?

The interviewer is a part-time postgraduate student studying for a research degree with the Centre for Computing and Social Responsibility at De Montfort University in Leicester, UK and is bound by that institution's ethical and disciplinary codes. The interviewer is also a network engineer employed in the aerospace industry however he is acting entirely in the capacity of student and *not in any way* in his capacity as an employee of any other organisation. Although this is unlikely, if you are aware of any potential conflict of interest which may arise from your participation please bring this to the attention of the interviewer.

Will you ask me about my company's IT security?

No, this is not the purpose of the study; the intention of the research is to understand the professional status of IT security management from the personal perspective of the interviewee and does not concern the security policy or practice of their employer. The only such information which may be requested will be:

- an overview of reporting structure (how your role fits within the overall management structure of your organisation and how IT security decisions are made), and
- your experiences of how your profession is seen within your organisation compared with other occupations of similar status, responsibility and skill.

Should however you wish to decline to answer any question to avoid revealing any commercially or personally sensitive information you are entirely free to do so.

Should you happen to use specific information from your current or a former organisation to illustrate a point it will be treated as confidential as described below, and you are free to request that whilst doing so the recording is paused and/or that the information not be used in the analysis. You are also able to request withdrawal of that information later as described below.

Can I withdraw?

Participation is entirely voluntary and your consent may be withdrawn at any time during or after the interview. Should you withdraw before the end of the interview or later but before any analysis has begun, all recordings and transcripts of the interview will be destroyed and this will be confirmed back to you when complete. No further use of any information provided by you will be made. Alternatively you may indicate that certain passages or responses should be removed, in which case these will not be transcribed (or removed from the transcription as appropriate) and these sections will not be used in the analysis.

Should you withdraw after the interview has been transcribed and analysis has begun, information from your interview may have already been combined with that of other participants to form theories and conclusions. In this eventuality, the recordings and transcripts of your own contribution will be destroyed and take no further part in the analysis, however it may not be practical to remove those theories and conclusions which were based in part on your information. In these circumstances, all reasonable efforts will be made to remove data from your interview from the analysis.

How will you handle my data? Will my contribution be confidential?

Recordings will be transcribed as soon as possible after the interview and the original media then deposited in a secure location. Once the interview has been transcribed and the accuracy of the transcription confirmed by the interviewee, the recording media will not be accessed again unless the examiners wish to check the quality of the transcription process. On completion of the project (in other words when the work has received its final pass or fail assessment) all materials other than the submitted dissertation will be destroyed.

Each person participating will be assigned an anonymising code which is used to identify their data during analysis and in the dissertation. This code contains a serial number and markers of length of experience and job role. Thus, once the data has been transcribed it will no longer be personally identifiable by anyone other than the student and his supervisory/examination team. Likewise, the name of your organisation will be removed from the transcript and replaced with an identification code during analysis which specifies only its approximate size and industry sector. Any excerpts quoted will be edited to ensure that the identity of the speaker cannot be deduced from the context.

If your employer requires access to a transcript of the interview as a condition of granting access, this will be explained to you beforehand.

Why use codes- why not remove all identifying data?

Firstly so that you can be sent your own transcript for verification. Secondly, it may be necessary to identify and remove the contribution of someone who later withdraws from the study.

What will my contribution be used for?

Information – once transcribed, anonymised and analysed – may be presented in the student's dissertation (and/or academic journals or conference posters or presentations) to support an argument or conclusion, or to demonstrate examples of opinions observed. This may take the form of verbatim quotes or as summarised, interpreted or paraphrased text, numbers, tables or other formats. This information may be attributed to the source, if so this will be by serial number, pseudonym or terms of the information listed above, i.e. job role, length of service, employer size and industry sector, never the identity of the participant.

Consent

I agree to participate in the research for the purposes described above. I understand that my participation is voluntary and that I can withdraw at any time and without giving a reason. I am eighteen years of age or older.

My organisation has requested access to the transcript of the interview and I expressly consent to this/

My organisation has not requested the transcript and will not have access to it*.

Signed _____ Date _____

Name _____

**Please delete as applicable*

Semi-Structured Interview Protocol: Academic in Information/Computer Security Field [1 of 5]
Version 1.0
Target Time: 90 Minutes

*Notes: Ensure that the consent form is signed before beginning.
It is expected that any non-disclosure agreements will have been signed before this point.*

1) Introduction and Housekeeping

*Thank the interviewee for their time.
Explain the purpose of the research in general terms (without seeding answers if possible).
Confirm if any points from the participant notes require explanation.
Reiterate the presence of the recording device, confirm consent & switch it on.*

2) Career Background

a) Could I ask you first, what is your career background? How did you come to be in this role?

Notes: This should serve partially to relax the participant thus avoid unnecessary interruption, but attempt to concentrate on their original career, intentionality of entry into security, the reasons for it and the reasons for the creation of roles rather than too much detail about non-security-related roles.

*Probes: What was their original subject of study?
Are they a career academic or did they return from industry? At what stage?
What prompted entry into security specifically?
Did they enter the field by active choice or happenstance?
What led to the creation of any security roles before this one?*

3) Course Origins and Content

a) How long have you been running a dedicated security course here?

Probes: Had there been security content in any other courses?

b) What prompted its introduction?

*Probes: Who pushed for this, e.g. was it student interest, academics or the university?
Has security increased in prominence or importance? If so what caused this?
Which disciplines/faculties were involved in its creation?*

c) How much of the course content is technical? Are any non-computing topics covered?

*Probes: Is there a distinction between computer security or information security?
Do you cover such topics as legal aspects, standards, management systems, education of internal clients, risk management, ethics and so on?
How do you decide and review the syllabus?
Has that changed? If so, why?
How is the balance struck? Which factors are involved and who directs this?*

d) Is the course sufficient foundation for work in an entry-level post in an information security team?

*Probes: Are any "soft skills" required? Are any needed for later senior roles?
Do you attempt to teach those?
How do you keep the content up to date and relevant? Is it?
Does that task differ from other courses?*

4) Student Entry and Intention

a) What sort of people do you recruit as students?

*Probes: Are they chosen on pure academic ability alone or are there other factors?
Are they mid-career, pre-change or pre-career, for example?*

b) Which roles will your students typically take on? Are you training them for any particular role?

Probes: What is the target or ultimate position for their career? Where could they go?

c) Do your students see security as exciting or glamorous?

Probes: Do their perceptions of the occupation change during their course?

d) Do well-reported breaches or events have any effect on your applications process?

Probes: If not is this because applicants are unaware of them or unmoved by them?

5) The Role of Certifications and Qualifications

a) Some people suggest that many of the current holders of senior security roles were often educated before security-related degrees were introduced. [Seek agreement or dissent.] Do you think they suffered a disadvantage because of this?

Probes: What would graduate entry have given them?

b) How would you contrast obtaining an academic security degree with the process of passing industry qualifications such as the CISSP or CISM?

Probes: Do you see yourself as in competition with these certifications?

Notes: Not just "commercially" but also are they even seen as kin?

c) If the government were to make it mandatory to hold a qualification in order to practise as an information security professional, would you see that as a positive thing or a negative thing?

*Probes: At what stage would it apply?
Positive for whom- the profession or the population?
What would be the primary driver?
Is excluding "quacks" a factor?
Degree or certification?*

d) What will be the typical career path for CISOs in future? Where will they be recruited from?

*Probes: Higher education, specific qualification, membership of a body,
qualification period. Has this changed, will it change and what are the factors
affecting this?*

6) Professionalism - General

a) What do you think of when you hear an occupation described as 'a profession'?

*Probes: If they do not spontaneously give specific criteria, question this but do not
suggest examples (to avoid bias in answering later questions).
Request examples if not given.
If only doctor/lawyer/accountant given, query pharmacy or engineering.*

b) Do you consider information security to be a profession?

*Probes: Why/why not if answered as a closed question.
Is it distinct from computing/IT?*

c) Do you think that your students see information security as a profession?

*Probes: Why/why not if answered as a closed question.
Is the prospect of professional status important to them?*

d) Do you think people in general see information security as a profession? How do you think it compares to

occupations such as medicine or engineering?

*Probes: If not what factors do they see as relevant to this, can they explain any disparity?
Should the roles be considered equivalent? Is the situation described “right or wrong”?
Is this because of hierarchy, budget, number of reports, depth of the knowledge required or the actual role?
Has that changed?*

e) Is information security a graduate profession?

*Probes: Should it be? Will it be? Is it trying to be?
If not, what is missing?
Is this changing?*

f) Do you think the information security occupation is seeking to attain equal status to the more “established” professions?

*Probes: What evidence is there/why do they think that?
Do/would they support that? Is it justified?
Is it succeeding? Why/why not?*

7) Additional Points

That concludes all the questions I had prepared. Are there any points you would like to add at all or which occurred during the interview?

8) Wrap Up

Switch off the recording.

Thank the interviewee again for their time.

Explain that the transcript will be mailed to them to verify its accuracy.

Clarify what markings are required to ensure that it will only be opened by them personally rather than by an assistant.

Semi-Structured Interview Protocol: Security Credential Body [2 of 5]

Version 1.0

Target Time: 75 Minutes

*Notes: Ensure that the consent form is signed before beginning.
It is expected that any non-disclosure agreements will have been signed before this point.*

1) Introduction and Housekeeping

*Thank the interviewee for their time.
Explain the purpose of the research in general terms (without seeding answers if possible).
Confirm if any points from the participant notes require explanation.
Reiterate the presence of the recording device, confirm consent & switch it on.*

2) Historical Factors

a) Could I ask you first, briefly what is your career background? What did you train as originally?

Notes: This must be relatively brief and avoid unnecessary biographical detail.

Probes: What was their original subject of study?

What prompted entry into security and at what point?

Did they enter the field by active choice or happenstance?

b) How did you come to be involved with this organisation?

Probes: Was it for career/salary/etc. reasons or strong orientation with its goals?

c) Why do you believe this organisation was formed?

Probes: Had security become a more prominent topic? If so, what caused that?

Were there any negatives which needed to be corrected?

Why then- did anything in particular happen to cause it to be formed?

How has the practice of Information Security has changed over your career?

Probes: What factors caused those changes?

3) Social-Technical

a) Is information security a technical occupation?

Notes: This is deliberately open- do not expand on the question unless drawn.

Probes: Is there a distinction between computer security or information security?

4) The Role of Certifications and Qualifications

a) Is information security a graduate profession?

Probes: Should it be? Will it be? Is it trying to be?

If not, what is missing?

Is this changing? Why?

b) Do your credentials replace or complement a graduate education?

Notes: Not just "commercially" but also are they even seen as kin?

Probes: Do you see yourself as in competition with graduate certifications?

Why are these degrees needed and getting more popular?

c) Now that security degrees are becoming much more common at Master's level and even at undergraduate level, how do you think this will affect uptake of your credentials?

Notes: Trying to elicit whether they are in competition

Probes: Do you see yourself as in competition with graduate certifications?

d) How many credential-issuing bodies should there be?

*Probes: Is the status quo acceptable?
Who should win out if rationalisation is needed?
Should there be a "regulator" for the industry?*

e) If the government were to make it mandatory to hold a qualification in order to practise in information security, would you see that as a positive thing or a negative thing?

*Probes: Positive for whom- the profession or the population?
What would be the primary driver?
Is excluding "quacks" a factor?
Are there any negatives?*

f) What should the role of government be in the regulation of information security practice?

*Notes: Might be answered above.
Do NOT say "profession"*
Probes: Would it be useful if your institution had control over entry to the profession?

g) What will be the typical career path for CISOs in future? Where will they be recruited from?

*Probes: Higher education, specific qualification, membership of a body,
qualification period. Has this changed, will it change and what are the factors
affecting this?*

5) Professionalism - General

a) What do you think of when you hear an occupation described as 'a profession'?

*Probes: If they do not spontaneously give specific criteria, question this but do not
suggest examples (to avoid bias in answering later questions).
Request examples if not given.
If only doctor/lawyer/accountant given, query pharmacy or engineering.*

b) Do you consider information security to be a profession? Do your members see themselves as professionals?

*Probes: Why/why not if answered as a closed question.
Is it distinct from computing/IT?*

c) Do you think your members enjoy similar status to accountants and lawyers in their daily work?

*Probes: If not what factors do they see as relevant to this, can they explain any
disparity?
Should the roles be considered equivalent? Is the situation described "right or
wrong"?
Is this because of hierarchy, budget, number of reports, depth of the knowledge
required or the actual role?
Has that changed?*

d) Are you seeking to raise the status of the information security occupation to be equivalent to other professions? How does it compare at the moment?

*Probes: Where are the gaps? Are they just gravitas/time or are they CBK?
Are they succeeding? Why/why not?*

6) Additional Points

That concludes all the questions I had prepared. Are there any points you would like to add at all or which occurred during the interview?

7) Wrap Up

Switch off the recording.

Thank the interviewee again for their time.

Explain that the transcript will be mailed to them to verify its accuracy.

Clarify what markings are required to ensure that it will only be opened by them personally rather than by an assistant.

Semi-Structured Interview Protocol: Government (Central/Policy) [3 of 5]

Version 1.02

Target Time: 75-90 Minutes

*Notes: Ensure that the consent form is signed before beginning.
It is expected that any non-disclosure agreements will have been signed before this point.*

1) Introduction and Housekeeping

*Thank the interviewee for their time.
Explain the purpose of the research in general terms (without seeding answers if possible).
Confirm if any points from the participant notes require explanation.
Reiterate the presence of the recording device, confirm consent and switch it on.*

2) Career Background

a) Could I ask you first please, if you are able from a security point of view, to tell me briefly about your career background? How did you come to be working in security?

Notes: This is aimed mainly for the demographics record to establish what background this person happens to have and to establish a conversation. Do not dwell on this at the expense of later topics. Be aware that this subject may also be sensitive if this person has come through the ranks in the security services.

*Probes: What was their original subject of study?
Are they a career civil servant or did they come from industry/academia?*

b) What caused your current role to be created?

*Probes: Are they the first person to perform this role?
Was it formed because of action from within the department or through the actions of an external party?
Was any other agency or department looking after this before?*

3) Security Practitioners

a) Is information security a technical occupation?

Notes: This is deliberately open- do not expand on the question unless drawn.

Probes: Is there a distinction between computer security and information security?

b) Is there a shortage of information security practitioners?

*Probes: If so, why?
Why now, what caused this to be a problem now?
How long has it been in place*

c) [IF B=YES] What sort of people are needed in the industry?

Probes: Are the roles for technical specialists or policy writers?

d) What will be the typical career path for school leavers in security?

Notes: Do not seed answers but follow up specific points mentioned in more detail.

Probes: Has this changed, will it change and what are the factors affecting this?

4) Certifications and Qualifications

a) Why did you introduce the CCP scheme?

Probes: *What was missing from the existing certifications dating from the 1980s?*
Does CCP status complement or replace the existing certifications?
Is the priority to establish a benchmark of competence or raise status?

b) The CCP can be assessed by multiple certification bodies. How many such bodies will there be in the future? Is there an ideal number?

Probes: *Is the status quo acceptable?*
Who should win out if rationalisation is needed?
Who will decide this?

c) Why has CESG begun the scheme to assess the quality of Master's degrees?

Probes: *Who should control the content of university security courses?*
Will you make compliance compulsory?

d) Is information security a graduate occupation?

Probes: *Should it be? Will it be? Is it trying to be?*
If not, what is missing?
Is this changing? Why?

e) How would you contrast obtaining an academic security degree with the process of passing industry qualifications such as the CCP, CISSP or CISM?

Probes: *Are universities in competition with these certifications?*

Notes: *Not just "commercially" but also are they even seen as kin?*

5) Professionalism

a) What do you think of when you hear an occupation described as 'a profession'?

Notes: *If they do not spontaneously give specific criteria, question this but do not suggest examples (to avoid bias in answering later questions).*
Request examples if not given.

Probes: *Is a profession regulated? How? Why?*

b) Do you consider information security to be a profession?

Probes: *Why/why not if answered as a closed question.*
Should it be? Does it have the required depth of knowledge?
Is it distinct from computing?
How wide is the profession- are a firewall engineer and a security awareness trainer part of the same profession for example?

c) Do you think the information security occupation has equal status with engineering, nursing or teaching?

Probes: *Why is that?*
Is that justified?
If no, where are the gaps? Are they just gravitas/time or are they CBK?
Note "are you seeking to change this" is the next main question.

d) Are you seeking to raise the status of the information security occupation to be equivalent to other professions?

Probes: *Why? (either way)*
 Is anyone else doing so?
 Are they succeeding? Why/why not?
 Would you help them? How?

6) Regulation

a) Does information security need regulation? Does it need for example a similar body to the Law Society or the General Medical Council?

Probes: *Should membership of such a body be mandatory?*
 Should anyone control entry to the profession?
 At what career stage would mandatory membership apply?

b) What should the role of government be in the regulation of information security practice, if any?

Notes: *Might be answered above. Do NOT say "profession"*

Probes: *Should government control entry to the industry?*

c) The government has arguably been active in the field of encouraging people into information security; do you think the NHS or DoJ would do something similar in medicine or law if there were shortages?

Probes: *Would you have taken this action had there been a full professional body?*

7) Additional Points

That concludes all the questions I had prepared. Are there any points you would like to add at all or which occurred during the interview?

8) Wrap Up

Switch off the recording.

Thank the interviewee again for their time.

Explain that the transcript will be mailed to them to verify its accuracy- ensure details are in place for this as this particular interview transcript must be agreed before analysis.

Clarify what markings are required to ensure that it will only be opened by them personally rather than by an assistant.

Interview Guide: Security Practitioner [4 of 5]
Draft 1.02

*Notes: Ensure that the consent form is signed before beginning.
It is expected that any non-disclosure agreements will have been agreed before this point.*

1) Introductions

*Thank the interviewee for their time.
Present a very short biography but do not align with or against IT Security.
Explain the purpose of the research in general terms without biasing. (3)
Confirm the interviewee agrees with the size and industry sector codes assigned.
Explain the presence of the recording device, confirm consent & switch it on.*

2) Career Path

a) "I'd like to talk about your career and how you came into your current role. Could you talk me through your career since leaving school and what led you to become a security practitioner?"

Notes: This is designed to be a straightforward first question to relax the interviewee, thus provide suitable non-verbal feedback, but as a narrative question avoid interruption.

3) Professionalism - General

a) "Could you describe for me please what you think of when you hear the term 'a professional'"

Notes: Ensure use of "a" to stress the noun rather than the adjective.

Probes: If they do not spontaneously give specific criteria, question this but do not suggest examples (to avoid bias in describing their own status later).

*Request examples if not given
if only doctor/lawyer/accountant, mention pharmacy or nursing.*

Is it a positive or negative term for this person?

b) "Do you think that people in general want to be thought of as professionals?"

*Probes: Follow yes/no with "why would you say that is" or similar.
Allow spontaneous answers then question status/cachet, power, salary.*

4) Professionalism and Status - Security

a) "Do you consider your own role to be a professional role?"

*Probes: Why/why not if answered as a closed question.
Are professional status and influence important and/or useful?*

b) "Do you think others see it as a professional role? In your organisation for example, would you say that your role carries equal weight to someone like a financial accountant or legal counsel?"

*Probes: If not what factors do they see as relevant to this, can they explain any disparity?
Is this because of hierarchy, budget, number of reports or the actual role status?*

c) "Has that changed at all? Does your role have more status or influence than it did ten years ago?"

Probes: What caused the change, but do not suggest specific examples if possible.

d) "Do you think that academic qualifications are important in your role?"

Probes: *Have they seen advertisements for these?*
 Are they required to gain employment or advancement?
 Are they substantial/"worth anything"?

e) "How about industry qualifications? Do you think those are useful or important?"

Probes: *As above.*

If not answered in (e):

f) "Do you have any of these qualifications yourself?"

g) "Why did you decide to pursue [that/those]?"

5) What is Security

a) "Do you think of information security as being a part of IT, like software development or database administration, or is it separate?"

Probes: *In what ways is it separate? [if applicable]*

b) "Is an IT security officer role primarily a technical position?"

Notes: *Offer "Which is more important to a company, its firewall or its security policy?" if the question is not understood.*

c) "Ideally, whom should the security manager report to in an organisation?"

Probes: *What are the reasons for this?*

If within IT hierarchy:

d) "Do you think there is a danger that the IT Director might over-rule the security team for operational convenience or to keep budget down?"

Probes: *Is that a bad or a good thing? Who **should** have the final say?*

e) "Does your role involve educating people? Is that important?"

Probes: *If no, establish whether this is because it is a colleague's role or that it's not performed at all.*

f) "Whose responsibility is it to ensure that the company's information is secure?"

Probes: *Roles of Board, CEO, CIO, users.*

g) "Overall, thinking about what we've discussed, what do you think the ideal education and career path would be for a security professional?"

Probes: *Higher education, specific qualification, membership of a body, qualification period.*

6) Origins

a) "During your career, have you ever been employed at an organisation where a new security-related position was created, like a security manager role?"

"yes" b) "Could we talk more in depth about that development then - could you talk me through what you saw as being the reasons why the position was created? Can you remember whether this was a response to something in particular or was it a gradual process? How did it come about?"

Notes: *Designed to elicit a narrative. Try to encourage a substantial story without interruption.*

"no" c) "Thinking of your own role then, why do you think that came about- what do you think might have caused the role to be created?"

Notes: *As for (b).*

7) Additional Points

Switch off the recording

a) “That concludes all the questions I had prepared. Are there any points you would like to add at all?”

8) Wrap Up

Thank the interviewee again profusely for their time.

Explain that the transcript is usually mailed to them to verify its accuracy, is this acceptable or would they prefer not to receive it.

If they are to receive a transcript ensure what markings are required to ensure that it will only be opened by them personally rather than by an assistant.

Interview Guide: Security Practitioner [5 of 5]

Version 1.1

Target Time: 80 Minutes

Notes: Ensure that the consent form is signed before beginning.

It is expected that any non-disclosure agreements will have been agreed before this point.

1) Introduction and Housekeeping

Thank the interviewee for their time.

Explain the purpose of the research in general terms without biasing answers

Confirm the interviewee agrees with the job role, organisation size and industry sector codes assigned.

Confirm if any points from the participant notes require explanation

Explain the presence of the recording device, confirm consent & switch it on.

2) Interviewee's Career Path and Motivation for Entry into the Occupation

a) The first question is about the choice of security as a career- what did you train as originally and how did you come to be in security?

Notes: This is intended partially to relax the interviewee and allow them to become more comfortable talking around a familiar subject, thus provide suitable non-verbal feedback, but as a narrative question avoid interruption early on in the answer.

Probes: Attempt to identify and draw out any specific factors which led to the establishment or expansion of security departments or resources, avoiding questions about their employer's current security arrangements.

3) Factors Affecting Change

a) Thinking back over your career, do you perceive information security as a business topic to be treated more or less seriously than before or has there been no change over that period?

Notes: determine whether any change is in business perception or resourcing.

If change has occurred:

b) What factors would you say have contributed to that?

Notes: Do not offer specific examples apart from to clarify the question until no further spontaneous examples offered.

c) Have the resources that are put towards it changed to compensate?

d) During your career, have you ever been employed at an organisation where a new security-related position was created, like a security manager role?

Notes: To be adapted according to the answer given in (2)

If "yes"

e) Could we talk more in depth about that development then. Could you talk me through what you saw as being the reasons why the position was created? Can you remember whether this was a response to something in particular or was it a gradual process? How did it come about?

Notes: Designed to elicit a narrative. Try to encourage the enumeration of factors without unnecessary interruption.

4) The Role of Certifications, Qualifications and Barriers to Professional Practice

a) I'd like to talk a little about the various academic and industry qualifications which are available in this

area. Firstly, do you think that academic qualifications are important in your role?

*Probes: Have they seen advertisements for these?
Are they required to gain employment or advancement?
Are they substantial/“worth anything”?*

b) How about industry qualifications? Do you think those are useful or important?

*Probes: Do you they have any of these qualifications themselves?
What was their motivation in doing so?
Is this different to an academic qualification and why?
Would they hire a CISO without one? How about a junior employee?*

c) You may have heard of the Government's CESG Certified Professional Scheme, which recognises some industry qualifications as meeting certain criteria for Information Assurance credentials. If the government were to make it mandatory to hold such a qualification in order to practise as an information security professional, would you see that as a positive thing or a negative thing?

*Probes: At what stage would it apply?
Positive for whom- the profession or the population?
What would be the primary driver?
Is excluding “quacks” a factor?
Could there be grades of qualification?*

d) What will be the typical career path for CISOs in future? Where will they be recruited from?

*Probes: Higher education, specific qualification, membership of a body,
qualification period. Has this changed, will it change and what are the factors
affecting this?*

5) Professionalism - General

a) What do you think of when you hear an occupation described as 'a profession'?

*Probes: If they do not spontaneously give specific criteria, question this but do not
suggest examples (to avoid bias in describing their own status later).

Request examples if not given.
If only doctor/lawyer/accountant given, query pharmacy or nursing.*

b) Do you consider your own role to be a professional role?

*Probes: Why/why not if answered as a closed question.
Is this status important to them?
Is it a positive or negative term for this person?*

c) Do you think that people in general want to be thought of as professionals?

*Probes: Why/why not if answered as a closed question.
Allow spontaneous answers then question status/cachet, power or salary.
Are professional status and influence important and/or useful?*

d) Do you think others see Information Security as a profession? Would you say that your role carries equal status to someone such as a financial accountant or legal counsel of equivalent experience?

*Probes: If not what factors do they see as relevant to this, can they explain any
disparity?
Should the roles be considered equivalent? Is the situation described “right or
wrong”?
Is this because of hierarchy, budget, number of reports or the actual role
status?*

e) Has that changed at all? Does your role have more status or influence than it did ten years ago?

*Probes: What caused the change, but do not suggest specific examples if possible.
What about regulation/statute/standards?*

f) Do you think the security occupation is seeking to attain equal status to the more “established” professions?

*Probes: What evidence is there/why do they think that?
Do/would they support that?*

6) Security in the Business

a) Do you think of information security as being a part of IT, like software development or database administration, or is it separate? Is an IT security officer role a technical position?

*Probes: In what ways is it separate?
Is there a technical/non-technical split?*

b) Do you think technical security staff aspire to be CISOs or security managers? Do you see them as being part of the same career?

*Probes: Are different skill sets required?
Do they make good CISOs?
Is there a glass ceiling for people without soft skills?*

c) Ideally, to whom should the security manager report in an organisation? Should they report to the IT director, for example?

*Probes: Examine both functional reporting line and grade.
What are the reasons for this?
Do they mention a conflict of interest in IT? If not, do they see one if asked?*

d) Whose responsibility is it to ensure that the company's information is secure?

*Probes: Do they own that responsibility?
Has this changed over time? Why?*

e) What is the effect, if any, of high profile security breaches reported in the media or of private ones within the organisation?

*Probes: Does this act as a lever to push/pressure senior management?
Does this assist with the credibility of the message?
Introduce standards as a comparison lever if not covered.*

f) What is the role of user education in Information Security?

*Probes: Is this done by technical staff or non-technical staff?
Is this a different skill set?
Is it important? Why?*

7) Additional Points

a) That concludes all the questions I had prepared. Are there any points you would like to add at all or questions you were expecting to be asked?

8) Wrap Up

*Switch off the recording
Thank the interviewee again profusely for their time.
Explain that the transcript will be mailed to them to verify its accuracy.
Clarify what markings are required to ensure that it will only be opened by them personally rather than by an assistant.*

[End of Instruments]

Appendix 2: Coding Frame Details

	No of Sources	No of Coding References	No of Words Coded
Category 1: Housekeeping			
I don't know	3	5	127
Interviewee Clarification	20	54	455
Interviewee Conversation	24	153	4182
Interviewee Housekeeping	9	14	152
Interviewer Clarification	24	123	1470
Interviewer Conversation	26	296	4783
Interviewer Housekeeping	16	53	1648
Interviewer Question	27	1271	41999
My thoughts on this subject are not fully formed	12	28	574
Not comprehended	6	8	123
Category 2: Certifications			
Sub-Category: Certifications - Academic vs Professional			
Academic study is or should be conceptual and timeless	5	18	940
Balance of technical and non-technical aspects	6	32	2017
CESG accreditation effort is assessed on commercial terms	2	8	311
CESG Accreditation is important as a validation of course quality	1	5	179
Comparison of academic and professional qualifications	13	20	1748
Factors affecting degree course content	5	15	781
Students gain real-life lessons from industry speakers	2	5	432
The role of formal university education in security	17	38	1814
Theory differs from or is inferior to real-life experience or skills	17	67	5118
Transition from study into paid work	2	6	334
Sub-Category: Certifications - Certifications Market			
Certification providers depend on candidate fees to survive	3	6	225
Competition and perception in the certification market	20	39	2527
Events prior to the launch of a certification	3	5	362

International considerations for certification	9	14	1110
Professional and academic qualifications are in competition	1	1	44
Professional and academic qualifications are not in competition or are complementary	6	13	1120
Recruitment of overseas students	2	2	45
Recruitment of students from current paid roles	2	5	231
Recruitment of students from school or university	4	8	265
The number of certifications	8	25	1645
We created our course to fit a demand in the market	5	11	660
Sub-Category: Certifications - Role			
Certification requires significant investment by the individual	4	9	464
Certifications are not an absolute prerequisite for employment	14	34	1463
Certifications are only needed when inexperienced	3	4	199
Certifications help demonstrate competence or give my voice weight	17	56	2874
Certifications prove commitment to standards to partners and customers	4	5	417
Certifications prove competence when changing role or applying for a position	19	64	3003
Current practitioners did not have the current range of training and certification options available earlier in their career	5	9	258
Experiences of pursuing certifications	13	26	1483
I couldn't enter security because I wasn't qualified to get the level or type of job I wanted	1	5	150
I regret not having a qualification which I could have got	3	4	248
My employer does not actively encourage me to undertake training or development	1	4	84
My employer encouraged me to undertake a qualification, or insisted	5	12	509
Undertaking a certification allows one to learn more about security	11	21	750

Category 3: Personal Aspects			
Sub-Category: Personal Aspects - Biography			
Active pursuit of security role or enhanced security content in role	5	5	240
Description of responsibilities, achievements and structure in a specific security role	17	52	4579
I observed or was attracted to security whilst working in a non-security role	15	32	2017
My career experience and skills do not yet justify a senior role	2	7	235
My interest in security developed pre-career	6	12	381
Pragmatism towards career direction or chance	16	35	2176
Security is exciting, challenging, interesting and rewarding	16	38	1492
Security learned 'on the job' on acquiring new responsibilities	5	8	635
Security staff originally trained in an unrelated discipline	24	37	2754
Security-neutral explanation of work experiences	10	60	4446
The effect of a suboptimal previous academic record	3	7	394
Sub-Category: Personal Aspects - Role Origin			
A combination of circumstances led to a requirement for increased security resource	4	4	252
I identified that there was a lack of security focus from outside	11	30	1213
My employer had a requirement to do something new	5	6	359
My position was new and I had scope to define my role	5	7	290
The increasing importance, focus or complexity of security caused a new role to be created	8	15	1074
The requirement for a security position was identified by an external party	1	2	28
Category 4: Professionalism			
Sub-Category: Professionalism - Definition and Characteristics			
I consider myself to be a professional	13	18	264
I do not recognise a distinction between professions and trades	8	9	601
I do not regard myself as a professional	2	3	70
Influential advisers must be credible	2	6	145

Ongoing training and continuing professional development	11	22	1432
Professional and professional titles are sometimes used too lightly	7	10	556
Professional is a negative term	1	3	136
Professional is a positive term	10	14	338
Professional means...	27	67	2236
Professional status brings duties and obligations, such as acting ethically	14	28	1168
Professional term definition includes formal and informal aspects	2	2	122
Professionals bring externally-derived standards into unique situations	5	6	352
Professions provide a benefit beyond increasing commercial profitability	2	4	229
Professions such as security must occupy a broad area of expertise with specialisations	4	7	786
Within a particular professional discipline there is a hierarchy of status	5	9	913
Sub-Category: Professionalism - Government			
Government departments cannot directly exert control themselves	1	2	31
Government keen to have a test of competence	2	8	599
Government should not directly regulate the market itself	4	10	832
Government wariness of imposing regulation	2	10	702
Government's main priority is public sector security	1	3	197
Sub-Category: Professionalism - Licensing			
Mandatory registration is not justified	7	15	1160
Mandatory registration must not exclude current competent people	7	13	387
Mandatory registration would have practicality challenges to establish a workable and equitable system	9	18	779
Mandatory registration would have resource implications	7	14	557
Mandatory registration would improve quality and be a positive step	20	42	1643
People in the occupation are generally competent	3	5	243
Some people in the occupation are not competent	6	9	251
The roles of professional association and regulator should be separate	1	4	185

Sub-Category: Professionalism - Status and Direction			
Background as a factor in security career progression	11	24	1425
Entrants to security are attracted by financial reward or career security	3	4	154
Fixed career paths are limiting or inappropriate	3	5	457
New entrants to a profession require a mentor	2	3	145
Professional status is associated with a capacity to do harm when incompetent	4	4	223
Professional status is important	5	8	203
Professional status is not important	4	7	264
Professionalisation is limited by lack of resources or will from powerful actors	2	6	311
Security career structure, status and comparison to other professions	19	65	4127
Security is not fully mature as a profession	12	23	947
Status is influenced by the individual not just the job	7	9	657
The availability of competent security professionals	6	10	454
The coherence of IT Security as a discrete occupation	11	34	1717
The future of the Information Security occupation	17	36	1581
The impetus for association came from within the industry	1	1	9
The professional status of the Information Security occupation	23	68	2591
Category 5: Work Context			
Sub-Category: Work Context - Change Actors			
Changes in the perception of security and its importance over time	20	51	3075
Networking as a source of information and influence	3	5	549
Security is a large and growing area of knowledge	5	8	343
The effect of changes in technology and connectivity	16	43	3313
The effect of customer requirements	3	6	240
The effect of industry sector and agility	11	30	1734
The effect of organised crime and foreign states	6	8	779
The effect of security breaches and the media	20	59	4615

The effect of standards, regulation and legislation	21	70	5843
The effect of supplier relationships	4	8	557
The effect of user behaviour and IT familiarity	9	21	1762
Sub-Category: Work Context - Enterprise Organogram			
Other Reporting lines for the CISO	6	7	458
Responsibility for specific security tasks may not be clear with well-known lines of demarcation	2	5	489
Security should not report to the CIO	11	26	1045
Security should or could report to the CIO	6	11	486
Security should report to senior or board management	12	27	1268
The effect of organisation size on security organisation structure	4	12	476
Sub-Category: Work Context - Intra-Professional Stratification			
Non-technical skills are career-learned	5	5	219
Non-technical skills should be taught alongside technical skills pre-career	2	3	140
Policy is empty without audit and enforcement	3	4	392
Possession of the correct approach and mindset is important	2	6	542
Security is a technical or computing discipline	3	10	400
Security is not exclusively or primarily technical	25	61	3859
Security managers need not be hands-on technical experts	14	27	1737
Security professionals must understand technology	11	19	1255
Security professionals need non-technical skills	12	34	2878
Some technical security staff do not aspire to non-technical or management roles	11	16	1215
The relationship between security and technical staff	7	18	940
Sub-Category: Work Context - Perception and Management			
As externals to the operations teams, security professionals can only advise	9	29	1731
Distinction between perception and substance	3	6	100
Security is an important thing to get right	6	10	477
Security is delegated by senior management as something which must be done	5	11	536
Security is not a priority for software companies	1	1	45

Security is perceived as difficult, blocking or not business-focussed	7	14	586
Security processes enabled the business to work more effectively	2	8	213
Security professionals may have to say no to protect their clients from harm	4	8	641
Security professionals must understand and live in the wider business	9	20	1160
Security-related decisions are a question of risk management and judgement	16	25	1601
The relationship between security and business management	13	46	2054
The role of a security-focused individual in the organisation	4	6	312
Sub-Category: Work Context - Users and Culture			
Cultural issues as a function of nationality	3	6	400
Educating people is an important part of security	15	49	3662
Ignorance of good security practice causes bad decisions and frustrations	1	10	487
Internal clients have their own priorities which are not necessarily aligned with good security practice	8	17	707
It is important to embed security into the culture as an accepted part of proper process	3	7	957
Policy and controls must be practical and not unreasonably affect efficient work practices	10	20	1442
Requirement to translate and empathise to enrol the non-technical	13	30	2659
Security is part of every role and not exclusive to specialists	15	35	1963
Ultimately some trust must be extended to the individual	6	7	280
User education is not practical, achievable or a priority	2	4	89

Appendix 3: Interview Codes and Details

Interview transcripts were assigned a working code using the following format: *AAABBC-DDEE/F*, where *AAABBC* identified the employing organisation, *DDEE* the person and *F* the serial number (in case the interviewee participates on more than one occasion).

AAA: Industry type. Many specific-purpose classification systems exist which are quantitative and complex with a particular aim in mind (Peneder, 2003) and may not include, for example, public and not-for-profit sectors if developed for capital markets. Since the research is intended to be carried out across many sectors in the UK, the general purpose UK Standard Industrial Classification of Economic Activities 2007 maintained by the UK government (ONS, 2007) was considered appropriate and adopted as the coding method. This scale assigns an arbitrary single character to each group; these original characters were recast as trigrams to be more human-readable during analysis. Those used are explained in the table below.

BB: A two-digit code was chosen to distinguish the organisation should multiple interviewees participate from the same institution. The number was randomly chosen to ensure that observers with access to the order of interviewing could not identify the source of a quotation.

C: Size of organisation. On the advice of the Office for National Statistics (*pers. comm.*, 30 October 2012 15:40) categories were adopted from those used by the Department for Business, Information and Skills (DBIS, 2012), viz: Small: 0 to 49 employees. Medium: 50 to 249 employees. Enterprise as 250 or more employees⁸.

DD: A code for the role or job title of the interviewee. No suitable existing set of codes could be located therefore this was constructed from roles observed during the literature review.

SM	CISO/Security Director or Manager
AN	Technical Analyst
CL	Course Leader (Academics)
ID	CIO/IT Director or Manager With Responsibility for Security
GV	(Single-use-class for Government)
DM	Deputy IT Manager
DS	Deputy Security Manager
PO	(Single-use-class for Professional Associations)

EE: A two-digit code to identify the participant, selected at random.

⁸ DBIS use “Large” instead of “Enterprise”, the latter being felt to be more common in the security industry.

The interviews were conducted as follows (* denotes pilot phase interviewee):

Interview Code	Date	Industry	Type	Protocol
CHA31E-SM07	Sep 2013	Charity	Practitioner	Pra 1.1
CHA33M-SM54	Sep 2013	Charity	Practitioner	Pra 1.1
COM73E-AN44	Apr 2013	Communications	Practitioner	Pra 1.1
EDU24E-CL05	Mar 2014	Academia	Educator	Aca 1.0
EDU27E-CL05	May 2014	Academia	Educator	Aca 1.0
EDU45E-CL31	Sep 2014	Academia	Educator	Aca 1.0
EDU54E-CL11	May 2015	Academia	Educator	Aca 1.0
EDU66E-CL71	Oct 2014	Academia	Educator	Aca 1.0
EDU79E-ID24*	Nov 2012	Academia	Practitioner**	Pra 1.02
ENT22E-SM03*	Oct 2012	Academia	Practitioner	Pra 1.1
FIN22E-AN43	Dec 2013	Finance	Practitioner	Pra 1.1
FIN31E-AN72	Aug 2013	Finance	Practitioner	Pra 1.1
FIN91E-SM15	Nov 2013	Finance	Practitioner	Pra 1.1
FIN99E-SM92	Apr 2013	Finance	Practitioner	Pra 1.1
GOV01E-GV01	Feb 2015	Government/Public	Cen. Government	Gov 1.02
GOV21E-DM38	Oct 2013	Government/Public	Practitioner***	Pra 1.1
HEL42E-AN12	Aug 2013	Health Services	Practitioner	Pra 1.1
MAN61E-SM05	Aug 2013	Manufacturing	Practitioner	Pra 1.1
MAN86E-DS66*	Oct 2012	Manufacturing	Practitioner	Pra 1.02
MIN48E-SM22	Mar 2013	Mining	Practitioner	Pra 1.1
PRO29E-PO42	Aug 2014	Professional Association	Professional Assoc	Pro 1.0
PRO41E-PO86	Nov 2014	Professional Association	Professional Assoc	Pro 1.0
PRO62E-PO74	Jul 2014	Professional Association	Professional Assoc	Pro 1.0
TEC11S-ID48	Jul 2013	Technology	Practitioner	Pra 1.1
TEC72E-AN91	Oct 2013	Technology	Practitioner	Pra 1.1
TRN74E-SM47	Apr 2013	Transport	Practitioner	Pra 1.1
UTL50E-SM62	Aug 2013	Utilities	Practitioner	Pra 1.1

**Although at an educational institution, this was an IT engineer with responsibility for security and not an academic.

*** Regional rather than central government.

Appendix 4: Transcription Rules as Used

- Transcription begins at the point that the first prepared question is asked (including the question); prior conversation is omitted.
- Transcription ends after the last response to the last formally-asked question including any immediately linked conversation.
- Each passage of speech by one individual is represented as a single paragraph terminated by two paragraph marks. No paragraph marks are used inside a passage of speech by one person however long.
- Short phrases which could compromise the speaker are (where practical) replaced by a grammatically compatible phrase in square brackets, e.g. “When I worked for Microsoft” would become “When I worked for [a large software company]”.
- If a substantial identifying section (i.e. more than a few words) is removed this is indicated with “[Identifying section removed]”; an ellipsis in square brackets is used for very small redactions.
- Where the exact wording cannot be made out this is indicated with “[indistinct]”.
- Italics may be used to represent heavy emphasis only where to do otherwise would give a misleading impression of their speech. They may also be used where word has been used demonstratively, such as in “They like *this* lemonade rather than *that* lemonade”.
- Where the interviewer is (by audibly laughing or by their inflection) clearly making a joke and without this knowledge the text would be misleading, this should be indicated with “(!)”.
- Where the interviewee anticipates and begins to answer during the reading of the question, provided it is not misleading to do so the text is represented as they had waited so that the question can be read in full next to its answer. If the response causes the interviewer to stop or trail off this is represented as “rabbits, would you do that or...” before starting a new section with the interviewee's response.
- Non-verbal noises are not represented, except where this would omit a response or be misleading, for example where the interviewee clearly agrees with something, which must be captured for analysis, but indicates only with “mmm-hmm”. In this example

this can be either rendered into text or represented as “[Yes]”.

- No attempt should be made to “correct” errors in syntax or grammar of the speech, however the desired result is a sentence which is comprehensible thus where absolutely necessary fragments of nonsensical or confused words are omitted.
- Where possible, where the speaker is imitating direct speech or reporting a conversation (real or in their view typical) grammatical conventions for direct speech are used.
- Abandoned phrases are removed unless they are substantial. Where the speaker tries to form a sentence and abandons their wording to attempt a different wording the fragment is omitted. Where a reasonably substantial part-sentence is spoken then abandoned then this should be represented, if necessary by indicating “...” at the point of abandonment. If the speaker actually corrects themselves then the corrected version is captured and the part they corrected is deleted. This is not indicated in the transcript. Care should be taken to omit phrasing which the speaker realised did not represent their view.
- Where the speaker has a very repetitive verbal tic which would make a completely accurate transcription more difficult to read and which is not relevant to the meaning of the text (such as repeatedly using “so”, “you know” or “like” not in their accepted grammatical senses) then this should be judiciously removed for clarity.
- Where the speaker uses conjunctions to continually link multiple sections of text so far that the sentence so produced is rather rambling, then this may be separated into sentences containing distinct and discrete concepts.
- Minor verbal prompts from the interviewer whose function is purely to indicate comprehension or elicit further answer text (such as “OK”) are omitted in order not to break up what are essentially continuous answer texts.