Conceptualising Adaptive Cyber Risk Management: Complexity, Rationality and Knowledge

Sallos, Mark

Award date:
2020

Awarding institution:
Coventry University

Conceptualising Adaptive Cyber Risk Management: Complexity, Rationality and Knowledge

By

Mark P. Sallos

PhD

September 2018

Conceptualising Adaptive Cyber Risk Management: Complexity, Rationality and Knowledge

By

Mark P. Sallos

September 2018

A thesis submitted in partial fulfilment of the University's requirements for the Degree of Doctor of Philosophy

Acknowledgements

Firstly, I would like to thank my director of studies, Dr. Alexeis Garcia-Perez, who has guided, supported, and resurrected this research on multiple occasions, and whose confidence and patience have both enabled and exceeded my own. I am also very grateful to my supervisor, Dr. Esin Yoruk, for her ongoing involvement, insightfulness and understanding.

I would like to thank Coventry University and CBiS for providing the resources, training and trust which have enabled my development as a researcher. I would also like to thank the numerous participants, collaborators and colleagues who have helped build and shape this project through their valuable inputs.

Finally, I would like to thank my wife and my parents who have always shown unwavering love and support, as well as my friends who have been an extension of my family. My gratitude far exceeds my (substantial) dislike for written expressions of affect. Love you all.

Pt. mama.

Abstract

The increasing reliance of organisations on ICT-enabled interconnectivity for value creation has redefined the boundaries and attributes of potential security vulnerabilities (i.e. causal intricacy, scope, non-locality and non-linearity). Cybersecurity presents an epistemic climate that is distinctly hostile due to its domain-specific dynamics, complexity, dichotomous objectives, and effect on behavioural tendencies. Within the thesis, the local manifestation of these dynamics is described as a heuristic – a 'knowledge problem'. This epistemic hostility hinders efforts to address and pre-empt the emerging threat of cybersecurity incidents in a manner that is proportional and contextually appropriate. The research argues that the degree of epistemic hostility faced by organisations, and its underpinning systemic and behavioural mechanisms, are inadequately represented in common inference-based constructs, like risk frameworks, which guide organisational practice, resulting in a 'context-construct gap'. Throughout the thesis, these premises are deconstructed, explored and addressed in three dimensions: a literature based, theoretical analysis focused on the interaction between risk, complex systems, and 'rationality'; an empirical, critical realist case study which explores and calibrates the postulated explanatory mechanisms in an illustrative real-world context; and a prescriptive formulation of an Adaptive Cyber Risk Management framework based on the theoretical and empirical findings of the study. The contribution includes a potential avenue for further cross-disciplinary enquiry into organisational cybersecurity management through the 'knowledge-problem' heuristic, which explores the pragmatic barriers to inference-based adaptation efforts. In addition, the Adaptive Cyber Risk Management framework proposes a conceptual logic to mitigate against the issues raised by the theoretical and empirical analysis, which include deep uncertainty, actor and decision maker bias, limited situational awareness, and systemic communication/coordination difficulties.

Table of Contents

1. Introduction ***9***

1.1 Context **9**

1.2 Framing: Problem Rationale **10**

1.3 Purpose **11**

1.4 Aim, Objectives and Roadmap **12**

2. Literature Review ***14***

2.1 Deconstructing a Knowledge Problem **14**

2.1.1 Macro Context 14

2.1.2 Uncertainty and Cyber Risk Management 18

2.1.3 Conceptualising 'Risk' 19

2.1.4 Cyber Risk: A Context-Construct Critique 22

2.1.5 The Cybersecurity 'Knowledge Problem' 26

2.2 Ontological Mechanisms: Systemic Complexity and Hierarchy **38**

2.2.1 Complexity, Metaphors and Mechanisms 38

2.2.2 Deconstructing Organisational Systems: Adaptive Cycles and the Panarchy 38

2.2.3 Order and Emergence 42

2.2.4 Evolution, Adaptation and Exaptation 46

2.2.5 First Principles of Adaptation 49

2.3 Behavioural Mechanisms: 'Rationality' and Social Adaptation **52**

2.3.1 Foresight and Intentionality: Reasoning and Inference Mechanisms 53

2.3.2 Pragmatic Rationality: Heuristics and Biases 55

2.3.3 Social Adaptation: Communication and Coordinated Representational Structures 60

2.4 Emerging Concepts: Towards the Conceptual Framework **65**

3. Methodology ***68***

3.1 The Conceptual Phase **70**

3.2 Research Philosophy: Contextualising Critical Realism **74**

3.2.1 Ontology 74

3.2.2 Epistemology 77

3.3 The Implementation Phase: Building the Methodology **80**

3.3.1 The Methodological Implications of Critical Realism 80

3.3.2 The Case Study in Cybersecurity Management 81

3.3.3 Hierarchy and Verticality: Case design 86

3.4 Data Evaluation: A Procedural Outline **98**

3.4.1 Engaging the Case 98

3.4.2 Data Collection and Management Overview 100

3.4.3 Data Management and Analysis 107

4. Case Study ***113***

4.1 Case Context: Sector Outline **113**

4.2. Case Data **121**

4.2.1 The Applied Dynamics of Cybersecurity Knowledge: University X 121

4.2.2. The Epistemic Substrate of Cyber Risk 130

5. Framework Development: The Strategic Knowledge Problem 144

5.1 Patterns of Convergence: Case and Theory 146

5.1.1 Ontological Complexity 146
5.1.2 Bounded Rationality 148
5.1.3 Cyber Risk Constructs 150

5.2 Formalising Adaptive Cyber Risk Management 152

5.2.1 Risk and Complexity: Heuristic Underpinnings 152
5.2.2 Adaptive Risk Management: Principles 153
5.2.3 Adaptive Cyber Risk Management: Situational Awareness Through a Knowledge Network 155
5.2.4 Accounting for Bias in Schema-Based Agents and Structures 159
5.2.5 Knowledge Claims as Adaptive Triggers 163
5.2.6 Knowledge Claim Parameters: Adaptive Risk Quantification and Meta-Cognition 166
5.2.7 Formalising an Epistemic Framework for ACRM 171
5.2.8 Framework Development: A Commentary 173
5.2.9 Framework Implementation Applicability 177

6. Conclusion 180

6.1 Objectives and Findings 180

6.2 Contribution and Implications 181

6.3 Limitations and Further Study 182

6.4 Research Journey 185

7. References 188

8. Appendices 205

Appendix 1: Informed Consent Form 205

Appendix 2: Participant Information Sheet 206

Appendix 3: Interview Topics and Questions 208

Appendix 4. Ethics Form 214

Appendix 5. A Risk-Centric Overview of Relevant Industry Standards & Frameworks 215

Appendix 6. Data Analysis Excerpt 218

1. Introduction

"It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox -- seen and unseen -- is something that we experience every day." (Obama 2009)

1.1 Context

Society is undergoing a technology-driven transition that is arguably unprecedented in its nature, scope, and scale. For organisations, both the proliferation and the democratisation of ICT have revolutionised the ways in which value is created and distributed through a tide of creative destruction which reshapes products, business models, corporate structures, and even markets on an ongoing basis. This phenomenon has accentuated competitive pressures by providing further incentives for technological opportunism and penalties for late adoption. But as companies compete to leverage the new dimensions of interconnectivity by immersing themselves in the "first manmade domain" (Kuehl 2009), they assimilate a growing base of vulnerabilities which are exploited by increasingly complex malicious actors (Kraemer-Mbula *et al.* 2013, Broadhead 2018).

Cybercrime is recognised as a key threat at both an individual (Goldberg 2016) and a societal level (Ferdinado 2015, UK Parliament 2015) due to its resulting streams of economic and societal externalities. However, as will be argued throughout the following chapters, organisations, as the fulcrum of the problem, are poorly equipped both conceptually and epistemically to deal with the distinctiveness of the uncertainty posed by the dynamics of cybersecurity. The significance of this problem is further amplified by the increasing stakes: a growing dependence on cyber infrastructure yields an ever-growing attack surface, further attracting threat actors who leverage the disproportional impact potential of the domain for the pursuit of economic or political agendas. (Bauer and van Eeten 2009)

In this emerging narrative, the role of supporting organisational cybersecurity is paramount.

Organisations drive economic value creation, own and defend stakeholder data, develop, manage and employ technical infrastructure. They are, thus, at the forefront of defensive efforts. Yet, locally, as function-specific systems, performance is primarily a function of the organisation's ability to efficiently create value in a manner prescribed by its operational model. The inclusion of cybersecurity in this existential context is both relatively novel and increasingly important. However, identifying how important is both an essential and a difficult exercise in foresight for organisations as they pursue pluralistic, at times competing objectives using bound resources which are leveraged through strategy.

1.2 Framing: Problem Rationale

Throughout the thesis, an overarching account of organisational cybersecurity will be provided through a strategic lens, as a function that is pragmatic, epistemic, inferential, dynamic, adaptive, and construct-assisted. Briefly, its pragmatism partly derives from its economic logic, where investments in security are largely supported by other primary functions and should not outweigh the potential costs incurred due to their absence. In addition, epistemological limitations and empirical grounding lead to the primacy of 'what works', rather than 'what's true'. Its epistemic, inferential status is central to proactivity — (appropriately granular) anticipation drives pre-emptive adaptation, which requires information, knowledge and inference. Its dynamism and, subsequently, adaptive status are a product of the perpetually changing adaptive pressures imposed by both external forces (i.e. threat climate, and compliance directives) and internal drivers (i.e. shift in strategy, systems, and behaviours).

Finally, the characterisation of organisational cybersecurity as construct-assisted is used to illustrate its reliance on normative representational and procedural constructs (i.e. frameworks, standards, methodologies) to frame its objects of analysis in a wider organisational context. The most prevalent example of this process is the notion of 'cyber risk'. Cyber risk assessments are pragmatic, aiming to encode the proportionality of likely outcomes, while structurally providing a common denominator for otherwise epistemically heterogeneous eventualities. They are also: epistemic, relying on a plethora of

informational/observational inputs; inferential as they describe non-observable events; adaptation-oriented, as they are used to treat, mitigate, or accept risks; and, potentially dynamic, based on their implementation. However, the pragmatic, adaptive value of such constructs is a function of contextual fitness at an implementation level. As a result, functional performance is linked to the congruence between the environment and the constructs used to identify and structure adaptive efforts. As heuristic/inferential procedures carry embedded assumptions about the environment of their use-case, incongruences can yield maladaptive behaviour, by distorting analytical outputs, compromising inference, and misrepresenting the actual uncertainty faced (Mousavi and Gigerenzer 2014). Both the potential for the misapplication of risk constructs, and its subsequent effects are illustrated in a variety of theoretical backgrounds (Aven and Zio 2011, Cox 2012, Mousavi and Gigerenzer 2014).

1.3 Purpose

The purpose of this research is to critically examine and conceptually address the tendency for a context-construct gap within organisational cybersecurity - cyber-risk applications. This exploration is conducted from the perspective of generative mechanisms and domain specific dynamics, which are identified as prescriptively[1] distinct/novel for organisational practice, and yield epistemic hostility — a knowledge problem. These include environmental complexity (non-linearity), social/behavioural dynamics, and domain-specific tendencies. In this context, the notion of a knowledge problem is used specifically to describe an epistemic barrier faced by organisations towards the effective inference-based identification and selection of adaptive pathways which adequately encompass cybersecurity. Based on this definition, locally addressing the context-construct gap entails mitigating the impact of the knowledge-problem as a precursor to epistemic diagnosis and adaptation. Throughout the following chapters, this narrative will be explored in three interdependent dimensions: theoretically, empirically, and prescriptively.

[1] [1] Throughout the thesis, the notion of 'prescriptive' is used to describe outputs which are practice-oriented, and procedural in nature – i.e. in the context of decision analysis, McFall (2015:46): "how real people *should* and *can* make decisions;". In this sense, 'prescriptive' is contrasted with 'descriptive' and 'normative'. Thus, the term is not used to denote rigidity or suggest a necessity for absolute interpretational fidelity.

In order to guide the analysis, a conceptual framework will be built based on the premise that inferential constructs in cybersecurity must locally account for the systemic dynamics, behavioural mechanisms and tendencies, as well as domain-specific epistemic barriers. As a result, achieving and sustaining context-construct fit is a function of managing the knowledge problem faced in a manner that is compatible with the previously introduced functional characterisation of cybersecurity. In other words, the narrative will argue that the use inferential constructs to pursue adaptive cybersecurity practice is hindered by an epistemic bottleneck. In this context, increasing the effectiveness of adaptive pathway identification efforts is a function of both the available knowledge, and its absence. Prescriptively, approaches for the navigation of the evolving threat landscape in a pragmatic manner must nurture epistemic adaptation while leveraging the variability imposed by the ontological mechanisms at play.

1.4 Aim, Objectives and Roadmap

In summary, the thesis aims to support the organisational cybersecurity context-construct fit by providing a better understanding of the context, and by correspondingly adjusting the construct assumptions and architecture. The first half of the thesis will deconstruct the 'knowledge problem' faced by organisations in managing their cybersecurity risks and provide an overview of systemic and cognitive mechanisms which underpin the context-construct gap. In the second half, an empirical investigation will be conducted in the form of an embedded, vertical case study. The outputs of this investigation coupled with the theoretical premises developed throughout the literature chapters will be used to conceptualise an Adaptive Cyber Risk Management framework/architecture as an epistemic, evolving interpretation of Cyber Risk Management. A visual representation of the thesis structure is presented in Fig. 1.

The structure reflects the following research objectives, which are further explored in section 3.1:

0. Construct a literature-based conceptual framework to represent the context-construct dynamics within organisational Cybersecurity;

1. Identify how Knowledge relating to Cybersecurity is produced, used and adapted at various levels within an organisation;

2. Critically analyse the role, and epistemic requirements of Cyber Risk Management;

3. Conceptualise a Risk based approach to address the Knowledge-Uncertainty dimension of cybersecurity management.

Section 2 serves as a de facto Literature Review, and integrates a series of literature-based chapters which provide an overview of the research context, introduce and consolidate the main structural heuristics ('knowledge problem' and 'context-construct gap'), discuss relevant systemic and behavioural mechanisms, and propose a theoretical foundation for the conceptual framework. Sections 3 (Methodology) and 4 (Case Study) introduce the research philosophy, empirical research strategy, and case study which, coupled with the preliminary framework introduced in section 2.4, address research objectives 1 and 2. They thus encapsulate the empirical dimension of the thesis which is instrumental the framework design process. Finally, section 5 explores the prescriptive implications of the research findings, which are used to formulate a theoretically compatible interpretation (a framework) of Adaptive Cyber Risk Management, and thus addresses the final research objective.

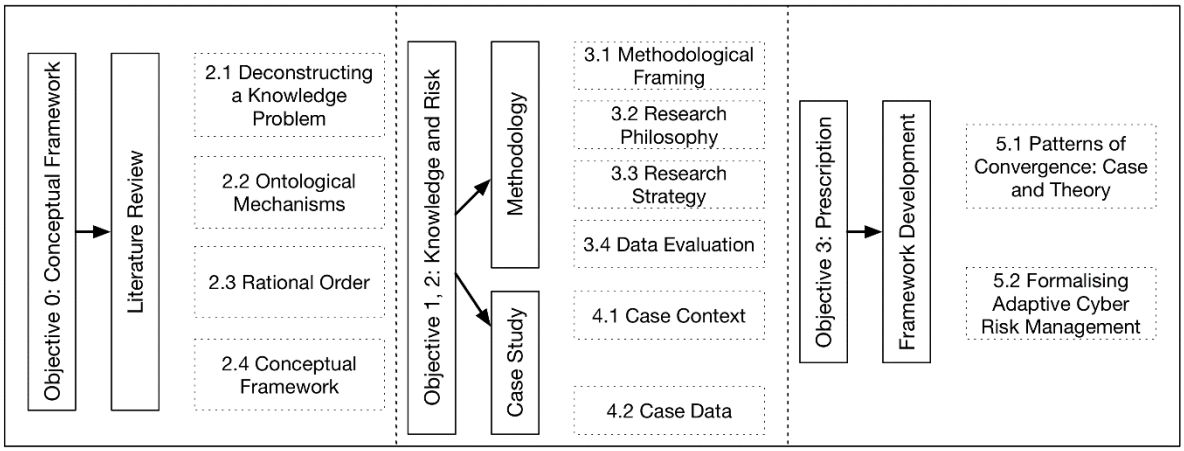


Fig. 1. A structural map of the research objectives

2. Literature Review

Throughout its four sub-chapters, the Literature Review aims to support the development of a conceptual framework which can illustrate and explain the dynamics of the research problem. In order to achieve this objective, the first part contains a literature-based analysis of the cybersecurity macro-context, which is used to highlight the contextual link between uncertainty and cyber risk. This is followed by a critical overview of the various literary conceptualisations of 'risk' in relation to their application context, and by an overview of tendencies and mechanisms which underpin what the project describes as a 'knowledge problem' dynamic — an inhibitor of the contextual utility/fitness of 'traditional' risk-based frameworks. Based on the first stage of literature analysis, two theoretical dimensions emerge as relevant and complementary in providing a mechanism-based representational structure to the research problem: systemic behaviour, from the perspective of complex, hierarchical structures; and 'rational' actor behaviour, from the perspective of cognition and social adaptation as drivers of action. These two theoretical dimensions suggest a series of complementary mechanisms which underpin the ontological regularities targeted by risk-based approaches through their emphasis on the likelihood and impact of incidents. Finally, the emerging conceptual framework is illustrated based on a relational representation of the chapter's core constructs. This output is also used as a 'logic-of-enquiry' for the construction and implementation of the empirical stage of the project.

2.1 Deconstructing a Knowledge Problem

2.1.1 Macro Context

When deconstructing the escalating importance of organisational cybersecurity, three trends stand out. The first is the rate of expansion and growing ubiquity of technology. In their 2009 study on connectivity trends, Cave et al. (2009) identified the emergence of an 'internet society' supported by an increasingly open communications infrastructure, the evolution of computing as a utility, and a growth in web intelligence which enables lower barriers between humans and computers. The popularisation of the Internet-of-Things (IoT)

and of 'always on' connectivity is generating an ever-growing footprint of technology and, subsequently, data which can be leveraged by organisations for both strategic and operational purposes (Bughin et al. 2015). Yet, this degree of technological omnipresence is a direct determinant of the attack-surface — the main space of potential interaction with cybercriminals. Despite evidence of amounting vulnerabilities (Greenberg 2016), the momentum of the 'internet society' seems stronger than ever. However, the spectrum of vulnerabilities emerging from this vector of societal change adds another layer of consideration for organisations, beyond their direct span of liability. As many consumers are also actors within an organisational setting, their personal vulnerability to cybercrime can spill over into their roles — an idea which blurs the line between personal and organisational cybersecurity. So, the growing reliance on the cyber domain has the unintended consequence of also expanding the 'habitat' of cybercrime.

The second noteworthy trend influencing the importance of organisational cybersecurity is the accentuated evolution of cyber threats. Nielsen (2012:340) defines the notion of 'Cyber Threat' as the product of (ill) 'intention and capability', which corresponds with the CIS (Computer and Information Security) notion of an 'attacker' (Kraemer and Carayon 2007). As the activity of the attacker/threat is generally illegal, the notion of cybercriminal is also used to similar effect. Kraemer-Mbula et al. (2013) argue that cybercriminal networks are exhibiting the characteristics of a digital business ecosystem, forming 'cybercrime ecosystems' focused on illicit value generation. The growing complexity and presence of cyber-criminal groups/nation-state supported actors operating in the space is also highlighted by the NCA (2018) in its strategic assessment of serious and organised crime. There are multiple ramifications which can be inferred from the existence of a cybercriminal market exerting pressures on its members. These include incentive driven behaviour, competitiveness and collaboration between actors, adaptivity to relevant policy and legislative measures designed to counteract its operations, balancing labour supply and demand, and an ability to exhibit macro level contraction and expansion based on the wider context. As performance-oriented structures which can leverage comparative advantages, cybercrime ecosystems can also adapt to market forces. This means that they can invest in research and development, incorporate external innovation into their practices, diversify their output based on effectiveness, and modify their structure to circumvent defences and

obstacles. Furthermore, peaks in the threat climate hostility are further accentuated by the emergence of specialisation-based cybercriminal value chain divisions (Thomas et al. 2015), lowered barriers to entry from a technology and know-how perspective due to 'off-the-shelf' malware, toolkits, and openly available guidelines for various attack vectors (Winter and Brunker 2014). As a result, in spite of defensive advances and increased awareness, threat dynamics presents mechanisms for adaptation and innovation, leading to increased offensive sophistication and potency.

The third trend is a function of the former two: the escalating impact of cybercrime. Visible high impact breaches are increasingly frequent. While only occupying a segment of the total number of incidents occurring (NCA 2018), they offer scarce insight into the scale of the problem, given the reluctance of organisations to disclose information on the topic, despite pushes from public policy and legislative bodies (US Congress 2015, NCA 2016), insurance companies (Association of British Insurers 2016), and academia (Casey 2004, Gal-Or and Ghose 2005). The 2015 Information Security Breaches Survey commissioned by the UK Government (PWC 2015) estimated that 90% of large organisations and 74% of SMEs suffered a breach in the preceding year. In contrast, the 2018 'Cyber Security Breaches Survey' notes that 72% of large firms, 64% of medium and 47% of small firms experienced a breach or an attack in the preceding year (GOV.UK 2018). It should be noted that the two reports present methodological differences and rely on declarative data. Also, breach/attack spread is a valid yet limited indicator of impact, as demonstrated by the significance of landmark events, such as the (US based) 2017 Equifax breach (White 2017, GAO 2018).

To anecdotally illustrate the financial vector of breach impact, Slaughter and May (2016) highlight the drop in share prices of a series of high profile UK and US public companies three days and a month after they reported a cybersecurity breach. The most dramatic decrease within the sample range was registered by Heartland Payment Systems — a security critical organisation — being recorded at -46.3% three days after the disclosure. The average price-drop a month after the breach for the sample of 9 companies cited in the study was -13.2%. While this measure of impact is by no means holistic or generalisable, it does illustrate how costly cybercriminal activity can be. As these drops follow the disclosure of incidents, they also provide insight into the rationale behind the reluctance of organisations to share breach

information.

Even apparently isolated incidents can, upon further investigation, reveal anecdotal evidence of the frequency and severity resulting from the interaction between evolving threats and a growing attack surface. The late 2014 Sony breach was noteworthy due to the amount of damage incurred, its media coverage and intentionally conspicuous attacker behaviour. However, Attrition.org (2014) documents tens of previous instances where the corporation, through its various operational branches, has been the victim of 'successful' and externally visible cyber-attacks. In response to the 2014 breach, Kevin Tsujihara, Studio Chief of Warner Bros. argued that: "[…] if someone is determined and spending the resources that [were] expended to try get into Sony, just about anybody's vulnerable, and you're seeing it in many different industries. The question isn't 'can you prevent it from happening?' […] I think, from what we've seen, the key thing is 'when it happens, what are you doing — how do you react?'…" (Chmielewski 2015). This perspective is consistent with the views of experts within the security community, who attribute a high probability of success to capable and focused threat actors (Schneier 2014).

So, given the dynamics of aggregate vulnerability, threat actor development, and the repercussions of breaches, the costs of cyber incidents are seemingly an almost unavoidable part of the modern operational climate (Romanosky 2016). However, the resulting dynamics are increasingly recognised, with attempts being made to mitigate their effect, as demonstrated by the financial support of cybersecurity solution providers. Investments in the field break year-on-year records, while the market is expected to reach a global value of $170bn by 2020 according to a Gartner report (Billings 2016). In spite of this, in 2015, it is estimated that 700 million records were stolen as a result of data breaches (Gemalto 2016). Due to several very high impact breaches, the 2017 estimates for this metric are significantly higher, reaching seemingly unprecedented values (Daitch 2017, Breach Level Index 2018).

The contrast between the consensus on the importance of cybersecurity (GOV.UK 2018), the increasing investments in the field, and the growing impact of breaches is counterintuitive. Yet, this disparity is persistent, and indicative of systemic tendencies and domain-specific dynamics. It delineates the uniqueness, the non-linearity, and the causal

disproportionality of the ever-changing cybersecurity context in which organisations operate. It also highlights a need for further supporting the development of locally evolving, adaptive approaches to organisational defence. Moreover, it highlights limitations in the efficacy of the conceptual tools used by organisations to frame and pre-empt cyber threats in their local context. Subsequently, organisations exhibit difficulties relying on foresight and inferential constructs in the pursuit of adaptive pathways. One of the main drivers of this difficulty is the uncertainty that characterises the domain. The following section will explore the dynamics between the organisational uncertainty presented by cybersecurity and cyber risk constructs.

2.1.2 Uncertainty and Cyber Risk Management

The most common construct-based approach for the mitigation of uncertainty and the coordination of cybersecurity processes, inputs, actions, and outlook is cyber risk management. Based on research conducted by PWC, 91% of the organisations sampled employ a risk-based cybersecurity framework (PWC 2016). Within the 2018 UK Cyber Security Breaches Survey data (GOV.UK 2018), 56% of business respondents have implemented some cybersecurity risk identification/assessment procedures in the preceding 12 months. The normative use of 'risk' to frame and describe cybersecurity situational assessment procedures in such reports is indicative of its status as a dominant paradigm.

Within the context of cybersecurity, Nielsen (2012:340) defines 'risk' as function of threats, vulnerabilities, and consequences, while proposing that its reduction can be achieved by supressing the presence of these three components. The Information Security Risk Management Standard – ISO/IEC 27005 –, defines risk as the product of the likelihood of an unwanted event, and the potential impact caused by an occurrence of the said event (ISO/IEC 2018). The two definitions can be used with complementary effect to illustrate the domain-specific interpretation of the concept, as Nielsen's (2012) expression of risk emphasises the three categories of variables which lie at the foundation of security risk thinking, while the ISO/IEC 27000/27005 definition illustrate the largely probabilistic nature of the concept (Nielsen 2012, ISO/IEC 2018). According to Hoo (2000:3), cybersecurity risk frameworks entail the assessment of risks through preference evaluation, which is established through the

estimation of the impact that can emerge from unwanted events, the likelihood of said events, and the evaluation of the attractiveness of potential courses of action.

So, the purpose of cyber risk frameworks is to minimise the effects of the uncertainty faced and to enable the pursuit of an active stance in influencing the nature and likelihood of foreseeable outcomes. This is achieved in broad terms through a risk management process which, based on the chosen methodology, defines a set of sequential stages which aim to define the context ("Frame" in NIST 800-39, "Context Establishment" in ISO/IEC 27005), identify and assess risks ("Assess" in NIST 800-39, "Risk Assessment: Identification, Analysis and Evaluation" in ISO/IEC 27005), act on the conclusion of the assessment ("Respond" in NIST 800-39, "Treatment/Acceptance" in ISO/IEC 27005), communicate the output of the process, and monitor and review its effects ("Monitor" and "Information and Communication Flows" in NIST 800-39, "Risk Communication and Consultation" and "Risk Monitoring and Review" in ISO/IEC 27005) (NIST 2011, ISO/IEC 2018). Risk management is also described by Hoo (2000) as a policy process with the aim of enabling decision making — more specifically, the formulation and selection of strategies addressing risk. A more detailed overview of the conceptualisation of Information Security Risk in relevant industry frameworks/standards, as well as their context and management processes is included in Appendix 5.

2.1.3 Conceptualising 'Risk'

In order to critically analyse the application of risk thinking in cybersecurity management, its inception and evolution are worth noting. The foundations of modern thought on risk are traceable back to the establishment of Probability Theory in the 17th and 18th century, which have provided a platform for the quantitative evaluation of cause and effect relations as a way to deal with uncertainty (Covello and Mumpower 1985, Zachmann 2014). 'Risk' has gained further prevalence throughout the 20th century as part of an attempt to deal with uncertainty in a mathematical, scientific manner (Zachmann 2014). The history of estimating and managing risk has been strongly shaped by developments in the ability to identify the variables which can be linked to unfavourable outcomes and are plausibly interpretable as determinants. Thus, the usefulness of the construct was consolidated by a growing body of

tools and techniques designed to establish and test causal links under uncertainty (Covello and Mumpower 1985). In many of the incipient applications of risk analysis, such as the health risks imposed by various occupations and practices, frequency data preceded and guided causal hypotheses which, once formulated, required testing before being usable to support the development of efforts to counteract said risks. (Dake 1992)

The heterogeneous nature of modern risk thinking is explored by Aven (2012), who distinguishes six evolutionary paths for the construct. These have emerged from the original perspective of risk as a function of expected loss/disutility and likelihood. In addition, they are interlinked by the presence of uncertainty, and the generally negative nature of the potential outcome. While also illustrating its modern societal role as the leading method of dealing with the uncertainty spectrum, Zachmann (2014) describes Risk as a subgroup of uncertainties which can be quantified through probabilistic measures. This implies a discrepancy between the construct's inherently confined probabilistic nature and its late-modern role in engaging most areas of uncertainty, and presents a point of potential conceptual divergence. Specifically, Aven (2017) notes that the concept, i.e. risk, should be distinguished from one of the ways in which it is measured, i.e. probability. In contrast, Mousavi and Gigerenzer (2014) present risk as distinctly probabilistic and differentiate decision making under risk from decision making under certainty or uncertainty. Furthermore, they present a typology of risk based on the means of employing probabilities: assessments based on a priori probabilities, which are known 'by design' given the parameters of the application system; statistical probabilities, based on experimental and empirical data extraction in conditions of ontological regularity; and, finally, assessments based on estimates, i.e subjective probabilities (Mousavi and Gigerenzer 2014, Beaudrie et al. 2011).

While primarily semantic, this apparent divergence can carry significant practical implications. Mousavi and Gigerenzer (2014) hold that the differentiation between Risks and Uncertainties is important given their different ontological status, and subsequent association to distinct evaluative/epistemic toolkits (i.e probability vs. heuristics/'ecological rationality'). In contrast, Aven's (2017) use of the term permeates the uncertainty spectrum, while recognising the effects of varying degrees of uncertainty on the adequacy of various

measurement/representational approaches. At the heart of this division lies the relationship between 'risk' and 'uncertainty'. Within the context of Risk, 'uncertainty' is defined by Haimes (2011:1178) as "the inability to determine the true state of a system". Furthermore, it is presented as a product of knowledge/its absence (epistemic uncertainty), and of randomness/ "emergent forced changes" (stochastic uncertainty).

Cox (2012:1608) proposes a taxonomy of uncertainty built around the ability to determine the system context, model, outcomes, and their weights. These parameters are spread over four levels, ranging from absolute determinism to total ignorance. Levels 3 and 4 are classified as 'deep uncertainty', with level 3 comprising of a context where the future is predictable in a multitude of plausible alternatives, there are multiple, varied system models, and the outcomes can be reduced to a known range (without definable probabilities/confidence intervals) with known weights. Level 4 is defined by the absence of knowledge in each of the four categories. Under deep uncertainty, the definition of risk presents a heuristic character where epistemic gaps or systemic randomness are counteracted through inferential 'rules of thumb' and procedural adaptation.

Thus, the philosophical, disciplinary, and implementation context of 'risk' can shape the fundamental approach used for its definition and application. For example, Aven (2012:34) highlights that, within logic and mathematics, risk is perceivable as a phenomenon which can be calculated, within medicine and science as an "objective reality", within sociology as "a societal phenomenon" and, within linguistics, as a concept. Subsequently, nine definitions are identified, equating risk to: 1. An "expected value"; 2. The "probability of an (undesirable) event"; 3. "objective uncertainty"; 4. "uncertainty"; 5. "Potential/possibility of a loss"; 6. "probability and scenarios/Consequences/severity of consequences"; 7. "event or consequence"; 8. "consequences/damage/severity of these + uncertainty"; and finally, 9. "the effect of uncertainty on objectives" (Aven 2012:37). The various dimensions encompassed by the definition of the concept reflect the variability in the emphasis placed on the components of the construct in different disciplines.

Out of the nine definitions, the sixth reflects the definition that is broadly used within cybersecurity management, as described in the previous section, and in Appendix 5. Based

on this interpretation of the concept, the effectiveness of a risk management implementation is reflected by its ability to accurately identify (anticipate) and (probabilistically) assess the risks faced in order to generate strategies that optimise the balance between the likelihood and the potential impact of a specific undesirable incident based on an understanding of its causal nature. However, beyond this high-level abstraction, the actual type of uncertainty that is faced within an application setting can have at least as much of an impact on the results of the process as its design (Aven and Zio 2011). As a result, a critical perspective on the role and the effectiveness of risk as a pragmatic construct must be anchored to a defined application-setting/problem-area, and subsequently, its uncertainty context.

2.1.4 Cyber Risk: A Context-Construct Critique

In the absence of clear patterns, sufficient data, and an accurate understanding of the causes which underpin undesirable outcomes, the pursuit of a (probabilistic) risk management framework can be detrimental as a source of false confidence (Aven 2013). In the context of impact assessment, Bond et al. (2015) approach risk as separate from uncertainty, ambiguity, and ignorance. This choice is justified by highlighting that "…a narrow focus on risk […] inadequately considers incomplete knowledge and can therefore lead to decisions that ultimately prove to be poor" (Bond et al. 2015:98). But knowledge sufficiency within the context of a given risk is also dependent scale of abstraction. Aven and Zio (2011) argue that in practical settings, systems cannot be described in totality due to an imperfect knowledge concerning the underlying phenomena, an idea which is tightly connected with the notion of scale of representation. Based on this premise, knowledge constraints can be masked from a process perspective through the alteration of the scale, or level of abstraction of the risk model.

The detrimental effects of inadequately representing the strength of the background knowledge in a risk setting are also addressed by Bjerga and Aven (2015:76), who acknowledge that, especially when facing deep uncertainty, probabilistic measures are "hard to justify". These premises are explicitly addressed within the literature as either points delimiting the applicability of the risk construct for specific types of uncertainty, or as critique

towards the misapplication of risk principles. Cox (2012) asserts that risks in circumstances of deep uncertainty lack a generally accepted set of decision models, while imposing one can oversimplify the analysis. (It should also be noted that 'defence against cyber criminals' is explicitly presented by Cox (2012) as an example of risk management under deep uncertainty.)

The domain-specific hostile epistemic dynamics, which will be covered at more depth in the following section, yield a common 'over-reliance on intuition' for cybersecurity decisions (Julisch 2013). However, decisions based on intuition can be masked within the apparent rigour of a well-established methodology. Once adopted, risk processes structure and potentially normalise analyst inputs and assumptions, yielding assessments which are inferential, and pertain a quantitative logic (i.e. enable comparison). Subsequently, the models assimilate subjective influences from their author (Haimes 2012), while the outputs of risk analysis are malleable, especially in their contextualisation. The potential scope of subjective inputs in cyber risk efforts is noteworthy given that the use of available data to effectively determine and alter networked (i.e. with non-local interdependencies) causal chains, through measures of likelihood and impact, can prove to be difficult within the uncertainty dynamics of cybersecurity management; especially when considering pluralistic organisational objectives and limited resources. For instance, cyber vulnerabilities are contingent upon a wide range of factors, including choices in infrastructure, operational models, technological systems, investment policy, corporate strategy, human capital, culture, training, and capabilities. As a result, the management of such a complex and dynamic causal network can be prone to oversimplification/distortion through single vector measurement, abstraction and modelling. The heterogenous epistemic nature of the individual eventualities (cyber risks) that are subjected to direct comparison under risk analyses is also worth noting. Without an embedded mechanism to reflect the nature of the knowledge used to identify and assess individual risks, the probabilistic output of the process can lead to decision making failures. (Haimes 2012, Aven 2013)

Given its heavy reliance on traditional risk paradigms, organisational cyber risk management faces several challenges which are imposed by the distinctive nature of the context/phenomena of concern. This issue is not novel. Hoo (2000) shows that several

'traditional' approaches to cybersecurity risk management share a propensity towards impracticality. This can occur in a number of ways, including through a tendency to reach unmanageable complexity of process and output, distortive simplification of the concepts employed, the use of ineffective metrics, or a reliance on non-existent or unrepresentative data which is argued to lead to methodological redundancy. Furthermore, the asset-centric object of information security risk assessments is criticised by Shedden *et al.* (2011), as it fails to account for organisational 'knowledge security'. Indeed, impact/outcome evaluation — a central component of cyber risk analysis/management — entails numerous complexities which are phenomenon-based and are difficult to consistently mitigate against locally through formal analysis processes (Thomas *et al.* 2013). These include: the inherent disincentives to disclose information concerning security breaches, difficulties in delimiting consequences and costs, intangibles and mis-estimated costs, consequences which are incommensurate, ambiguity, uncertainty, absence of information, and ignorance, near-misses, pluralistic interests, and bias.

In a broader context, Haimes (2012) notes a series of systems-based theoretical first principles for the effective use of risk (analysis, assessment, management), which provide a critical lens of analysis when considering cybersecurity as a use-case. Amongst said principles, a series of notable themes emerge. These include a necessity to incorporate/address holism, temporality, the inherent nature of conflicting and competing objectives, both epistemic and stochastic uncertainty, as well as the eventuality low probability/extreme consequences. Indeed, holism, temporal dynamics, heterogenous adaptive drivers, complexity, and phase transitions are all functions of ontological/systemic mechanisms which are likely to manifest themselves in a dynamic, complex, real-world setting. Estimating the likelihood and impact of an outcome must carry embedded assumptions about the scale-dependence of the effect (i.e. variation in the effects of a breach across the information system infrastructure, the organisation, the stakeholder network, the sector). Additionally, locally optimal outcomes can be holistically maladaptive (i.e. treating a cyber risk can impact overall operational performance).

The eventuality of phenomena and outcomes is temporality-dependent, as it shifts based on the dynamics of the systems. This aspect is amplified within cyberspace, given the nearly

instantaneous pace of interactions, and the decreased role of geographical boundaries. Both dichotomous adaptive pathways and residual uncertainty are inherent for organisational cybersecurity, due to the limitations of foresight in this space. Low-probability, high impact occurrences are also foundational to defensive efforts, given the scope of the 'unknown-unknown' and the significance of the potential impact. Based on the above measures, likelihood-impact risk constructs lack the inherent conceptual robustness needed to effectively respond to the environmental dynamics and ontological mechanisms that drive cybersecurity phenomena. Finally, given the extent of cognition as a driver of outcomes in organisational settings, there is also a need to incorporate an adequate representational mechanism/model to account for cognitive tendencies and social dynamics in matters of cybersecurity. (Haimes 2012)

So, within the current paradigm of assessing the likelihood and impact of (undesirable) outcomes, the contextual effectiveness of cyber risk approaches is conditioned by: the potential for adequate (in volume, quality, and availability) information concerning the potential outcomes; an ability to extract and employ the information for inferential procedures; and a (reasonably) linear environment. This logic is also applicable to non-probabilistic measures of likelihood. Even outside probability, the mechanics of inference used to describe potential/likely outcomes require an ontological regularity (a product of either linear or emergent dynamics), data to form a (series of) model(s) which captures its tendencies, and an inferential procedure to generate and employ an output that enables effective action. In contrast, the effectiveness of archetypical/traditional risk management is damaged by factors and dynamics which dilute its ideological utility: unpredictable outcomes due to epistemic scarcity, erroneous information, chaotic or complex systems/interactions, and a propensity for misunderstanding the causalities of significant events. The setting-specific occurrence of such factors indicates a context-construct incongruence. To further explore this narrative, the domain-specific epistemic dynamics will be deconstructed in the following section through a phenomenon-based view of organisational cybersecurity. An overarching argument will be made that organisations face a 'knowledge problem' which is simultaneously the source and a driver of the context-construct gap in cybersecurity management.

2.1.5 The Cybersecurity 'Knowledge Problem'

Throughout the thesis, the notion of a 'Knowledge Problem' will be used to describe a hostile epistemic dynamic which affects adaptive inference within the functional context of Cybersecurity Management. Subsequently, it overlaps with the previously introduced notion of 'uncertainty' as it can focus on factors which prevent determining the true state of a system. However, unlike uncertainty, which is defined as systemic (within the study), and reflects an epistemic state, a knowledge-problem describes epistemic tendencies, is a product of ontological mechanisms, and is anchored in a pragmatic, behavioural grounding. Thus, the 'knowledge problem' framing emphasises the role, attributes and tendencies of the locus of knowledge — i.e. the 'knower' — in relation to an evolving problem-setting. In order to break down the conceptual efficacy of using Risk Frameworks to tackle the organisational cybersecurity knowledge problem, the key trends which shape it as an application setting must first be explored.

Establishing the dimensions of a knowledge problem is a key step in its analytical breakdown and, implicitly, in the pursuit of potential responses. As a result, the following sections of problem analysis address the context-specific environmental complexity, available information relating to the context, and the social drivers affecting its assimilation and use for decision-making purposes, as indicators of adaptive inference tendencies within cybersecurity management. Following this chapter, the cybersecurity 'knowledge problem' context will be explored from the perspective of its underpinning mechanisms. Popper's three-world ontology (Popper 1978) is used to structure this line of enquiry, as an epistemological heuristic, indicating the locus of knowledge. Thus, a theoretical analysis of its systemic/'real world' component (World 1 - physical), and its social/'rational' component (World 2 — conceptual), will be developed as a bedding for empirically and conceptually exploring their 'objective knowledge' (World 3 — construct), pragmatic implications based on the attributes of the application context (Popper 1978).

2.1.5.1 Information: Source, Availability, Validity

The relationship between the cybersecurity decision making and its informational input is pivotal in ensuring an appropriate interpretation of the relevant problems that are faced. Within the context of quantitative risk assessments (probabilistic risk assessments), even at a high level of abstraction and simplification, obtaining the required information to compute risk factors effectively is not a clear process, as highlighted by Sommestad et al. (2010). The theoretical efficacy of probabilistic techniques of decision support is directly proportional to the underpinning sample size used, and to the fidelity of its represented attributes. So, a reliance on local breach data may be insufficient for the effective extraction of patterns, trends and likelihoods. Even internal insights may prove difficult to obtain objectively, due to limitations in awareness and capabilities. These limitations are manifested, for example, in the slow breach detection times, which have been argued to take an average of over 6 months, with significant industry-based variation (Osbourne 2015), and a median of 146 days (Mandiant 2016).

Subsequently, the importance of information sharing as an enabler of cybersecurity performance has been recognised in both academic literature and public policy for over a decade. For example, Gal-Or and Ghose (2005) argue that gathering, analysing and sharing data on both successful and unsuccessful security breach attempts are key components of improving security. This thesis is the premise of numerous cyber incident information sharing initiatives, which, particularly through public-private partnerships, are a reoccurring point of both national and international security policy. Just in the U.S, such initiatives include: PDD/NSC 63 (Clinton 1998); Section 225 of the HSA/Cyber Security Enhancement Act of 2002 (GPO 2002); the output of the 2009 Cyberspace Policy Review (White House 2010) and the subsequent 2011 legislative proposal (White House 2011); EO 13636 (White House 2013) and EO 13691 (White House 2015); as well as the National Cyber Strategy (White House 2018). Similar initiatives are also in place within the U.K, in the form of the 2009, 2011, and 2016-2021 Cyber Security Strategy (UK Government 2009, UK Government 2011, UK Government 2016); and in the E.U through the Cybersecurity Strategy for the European Union (European Commission 2013), and in ENISA's Information Sharing/Public Private Partnerships efforts

(ENISA 2019). The shared ambition of all these efforts to "bridge the gap" between organisations and national security bodies for the purpose of information sharing and support is in itself an indicator of both the importance of, and the reluctance towards/limitations of current breach information sharing.

Due to limitations in actionable information sharing, there is a strong dependence on data acquired from third parties which can collect, aggregate, and share/sell it based on their operational model. However, the opaque nature of the informational product, and the financial incentives of the sellers generate a market characterised by information asymmetries (Moore 2010). Akerlof (1970) introduced the notion of 'information asymmetries' to highlight the aggregate effects occurring as a result of actor dishonesty in opaque circumstances. This concept is applicable to organisational cybersecurity in a number of ways: as vendors sell solutions of a relatively opaque effectiveness, the pursuit of longer development cycles, or, in the case of threat intelligence, increased sample sizes and data collection efforts, can lead to a competitive disadvantage, absent a truth-telling mechanism, when compared to 'lemons' (inferior products that are overvalued in a transaction through asymmetric information). Similarly, as organisations benefit from opaqueness in relation to their security capabilities, consumers can only gain insight regarding said capabilities as a result of atypical occurrences, such as high-visibility breaches or 'whistle-blowing'. This affects the competitive feasibility of high investments in security, when having to compete with 'lemons'. So, the potential effects on market confidence, quality, price and competitiveness resulting from the unbalanced informational availability and dynamics between interacting parties are significant. (Anderson and Moore 2006, Romanosky 2016)

The implications of asymmetric information have been previously explored, particularly within the cyber intelligence market. In its report on 'Estimating the cost of cybercrime', The Economist Intelligence Unit (2013) presented the limitations of widely reported information concerning the aggregate economic impact of cyber-criminal activity by highlighting the major discrepancies found between existing assessments. In 2012, Symantec estimated a global cost of cybercrime to the economy of $110bn, which is significantly lower than the $1trn global cost approximation made by McAfee in 2009. McAfee's 2014 and 2018 estimates are comparatively more moderate and consistent ($400bn-$600bn), accounting for an

approximate $45bn year-on-year growth, yet still present a $200bn range between the 'conservative' and the 'maximum' values (McAfee 2014, McAfee 2018). While some inconsistencies between reports are to be expected due to differences in methodologies, sample sizes, and scope, the acute variation between values highlights the limitations of such information as a source of insight. This phenomenon is further exacerbated by the challenges presented for consistent, reliable data collection on cybercrime (Broadhead 2018). Nonetheless, such figures/estimates are influential in the public discourse.

Greenberg (2012) quoted two contributors to the studies containing the previously highlighted figures (more specifically the 2009 McAfee report, and the Symantec report suggesting that cybercrime leads to a cost of $250bn/year for American firms), who were surprised by the end outputs which they characterised as grossly exaggerated. However, in spite of its disputed status (Greenberg 2012, Economist Intelligence Unit 2013), the $1trn figure was quoted by U.S. President Barrack Obama (2009) as part of his speech addressing the importance of cybersecurity, and thus populated beyond its initial reach. Incorrect estimations of the effects of cybercrime at a macro level can misinform decision makers, or force them to speculate what adjustments should be applied to the available data, both instances leading to potential inadequate response strategies, over or underemphasising the evolving significance of the problem. They also affect the perceived credibility of third party information due to its susceptibility to distortion and overgeneralisation. Even parties that are not commercially vested can output misleading or untruthful strategic information, as highlighted by Ziv (1993), who argues that, absent a "truth telling mechanism", the gains obtained through private information sharing within oligopolistic circumstances are outweighed by the incentives of firms to misrepresent their position and strength.

Attackers are also likely to leverage informational asymmetries by speculating adversarial dynamics. Within cybersecurity, their position entails numerous inherent strategic advantages which include: having an active role (first mover), an ability to employ disinformation and leverage defender uncertainty (Prince 2016) and to gain real-world feedback concerning their offensive capabilities. In contrast, the defensive position is largely reactive, supported by pre-emption consisting of general anticipation, deterrence, and mitigation. In addition, it is also susceptible to misinformation and deception having limited

means to verify threat specific hypotheses which include a reliance on simulated defence for feedback (i.e. penetration testing/white hat hacking), anecdotal evidence, and retrospective analysis of prior attacks (which can entail inferences from incomplete information, non-actionable insights, or attack vector specificity). This asymmetry is further amplified by functional specialisation: attacker rent-seeking relies on offensive primary capabilities, while organisations, as defenders, are functionally conditioned by value generation through primary capabilities that are often dichotomous to security. All these factors play a role in the uncertainty faced by the actors, while also influencing the range of tools and mechanisms which can be used for its mitigation. Thus, due to the inherent informational and strategic disadvantages of the defensive position, such actors have to exhibit a higher efficiency and effectiveness managing the uncertainty they face.

2.1.5.2 Assimilating and Acting on Information

Beyond the availability of sufficient relevant security information lies the issue of its assimilation, contextualisation and use. For uncertainty to be effectively mitigated through predictive means, not only is sufficient valid information required, but insight has to be extracted from it and incorporated into an actionable format. When deconstructing the development of actionable insight/intelligence within cybersecurity, two interdependent aspects stand out: a capabilities, and a behavioural component. Reece and Stahl (2015) explore the cybersecurity aggregate capabilities availability gaps and development efforts at within the context of the UK market, with particular emphasis on governmental efforts aiming to stimulate such development through professional formalisation. The study illustrates the spike in demand for information security staff, citing a 74% increase between 2007 and 2013. The absence of a centralised, common body of knowledge, the evolving, context-dependent role requirements, as well as the emphasis on "experience and social factors over learned technical skills and graduate entry" are some of the barriers faced by centralised efforts to stimulate the supply of information security capabilities through "professionalisation" efforts (Reece and Stahl 2015:193). So, given this market context, as well as the novelty and inconsistencies of cybersecurity roles, it is clearly difficult to rely on the availability of tacit expertise and individual capabilities as a counterbalance to process inefficiencies and informational issues. An increasing cybersecurity skill gap is also identified by FireEye's (2018)

M-Trends report as a function of disproportionality between the rate of growing demand and the available supply.

In their investigation on the role of human behaviour in cybersecurity risk, Pfleeger and Caputo (2012) highlight the effects of bias and cognitive load limitations in the interpretation of security information (presented in the form of scenarios) by practitioners. It should be noted that the notion of 'practitioner' is used to describe participants to the study who have been selected based on their "decision making authority about cyber security products and usage" (Pfleeger and Caputo 2012:600). The findings of the study include a series of noteworthy conclusions, such as the lack of a shared understanding or distinct awareness of security amongst the participants, a failure to identify patterns and "connect the dots" when having to combine a narrow focus and a large volume of information, and a lack of experience in deconstructing situations in order to determine security relationships. The practitioners showed difficulties in their attempt to understand the nature of the risk presented in each scenario and evaluate multiple perceptions to determine the optimal decision within the time constraints — an issue accentuated by the high cognitive load (high stress applied to the working memory of the analyst), and discernible effects of bias. Biases are presented by Heuer (1999) as a common, yet highly detrimental factor affecting intelligence development.

In addition, Pfleeger and Caputo (2012) argue that security is generally perceived to be a secondary task, and rarely a goal in itself, which is an indicator of incentive misalignments. The detrimental effects of misaligned incentives and principal-agent problems on managing (general) risk are well documented, being described by Haldane (2009) as one of the main causes of the financial crisis of 2008. Moore (2010) highlights the multitude of incentive misalignments which emerge within cybersecurity because of the efficiency-security dichotomy. This issue is accentuated by the division between the risk faced by the organisation/system and that faced by individual decision makers and security actors. Subsequently, the misalignments occurring between the individuals and organisations tasked with ensuring security and the beneficiaries of such efforts, are characterised as "rife" by Moore (2010) who argues that stakeholder incentives should be the starting point in the analysis of cybersecurity. Pfleeger and Caputo (2012) discuss the tendency of users to subvert security measures and systems which impede on the ability to carry out the primary task. As

a result, the motivations of the stakeholders can have a significant effect on the information that is collected, its validity, and its assimilation within a narrative.

The literature barriers to effective cybersecurity/information security practice includes a variety of socio-behavioural factors. These include human errors (Kraemer and Carayon 2007), perception and bias (Kraemer 2009, Pfleeger and Caputo 2012) and the organisational culture (2006). In addition, Kraemer (2009:510) identifies a series of additional human and organisational themes which underpin cyber vulnerabilities: technology, management (including resources and performance management), policy problems, and training. Given their distribution throughout the organisational cybersecurity function, these factors condition both the foresight and the likelihood of incidents. Furthermore, they are a manifestation of both of the behaviour patterns and capabilities needed to assimilate information effectively across organisational roles in order to make adequate inferences. As a result, in order to tackle cybersecurity as a knowledge problem, there is a need for a more robust conceptualisation of social/behavioural mechanisms within the prescriptive constructs used.

2.1.5.3 Problem Context: Complexity and Foresight

The degree of complexity attributable to the context of a risk problem is arguably the most generalisable determinant of the utility gained from traditional risk analysis methods. High levels of complexity affect the feasibility of anticipatory scenario-building, convolute the system models, and limit the effectiveness of probabilistic analysis — all indicators of deep uncertainty (Cox 2012). In his analysis of cyberspace, Phister (2010) emphasises the importance of the differentiation between its classification as a complicated system versus a complex one, proposing the latter to be correct. Complicated systems are deemed to exhibit high levels of dynamism while incorporating many moving components. However, they also exhibit linear cause-and-effect relationships that allow the prediction of systemic behaviour and phenomena with significant confidence. In contrast, complex systems present nonlinear interactions between components, an absence of centralised control systems, self-organisation and co-evolution, as well as non-equilibrium order and collectivist dynamics. Thus, the pragmatic and epistemic implications of classifying a risk problem as complex rather

than complicated are highly significant. (Phister 2010)

Benbya and McKelvey (2006a:17) suggest that (dynamic, open) systems can exhibit three possible states: stable, chaotic and an intermediate state of "critical complexity", "emergent complexity" or "melting zone". They distinguish complex systems based on the significant strength of the interactions between their elements, which is manifested through the potential effects of current events on a wide range of probabilities associated with future events. Thus, in complex systems small changes and perturbations can lead to large, seemingly unrelated effects through nonlinearity. Mason (2007) presents increasing complexity as inversely proportional to predictability and environmental adaptation. Given the volume of perpetually interacting actors and components which define cyberspace beyond its physical infrastructure dimension, and the dynamism of its interactions, it can be seen as alternating between critical complexity and chaotic states (Kuehl 2009).

In this context, Sharma and Dhillon (2009) critique 'traditional risk analysis approaches' in Information Security, which are defined based on the premise that risk is quantifiable, due to their failure to accommodate the chaotic nature of the key variables and their context. The authors' interpretation of chaos theory overlaps with the complexity narrative through ideas such as nonlinearity and high degree of dependence on the initial conditions within a system, but proposes the employment of 'strange attractors', which are defined by Rickles et al. (2007) as a chaotic system's aperiodic, non-repeated patterns of configurations (phase-space points) manifested after recovering from perturbations. Chaotic systems are distinguishable from other complex systems in that they are not defined by the volume of interacting sub-units, but by the intricacy of the dynamics which results from their interaction (Rickles et al. 2007). Subsequently, complex systems can be chaotic, and chaotic systems are complex, yet the two are not equivalent. Despite the seemingly chaotic nature of security incidents, as manifested through their aperiodic occurrence and intricate dynamics which emerge from the permutations of rational adversarial behaviour and the dynamic asset-vulnerability base, the broader complexity construct presents itself as a more robust conceptual foundation for ontological/stochastic deep uncertainty within cybersecurity. While acknowledging the potential for oscillation between states of critical complexity and chaos, asserting that cyberspace — especially at a defined, organisational level — is inherently chaotic is hard to

justify. Nonetheless, if nonlinearity is recognised as a mechanism that shapes the ontology of cybersecurity, there are significant implications for the inferential paradigms and constructs used for decision making. (Gershenson 2013)

The centrality of scale and granularity when discussing complexity and cybersecurity events is made apparent by the characterisations of complex systems. For example, Phister (2010:15) presents five components of complexity within systems. These are:

- Complex and networked causality in the absence of simple cause-and-effect relationships;
- Vast volume of plausible options which make the system impossible to optimise;
- The behaviour of the system exhibits recurring trends and patterns;
- Pattern and trend variation due to the co-evolutionary process, the absence of equilibrium-based order or centralised control systems; and
- Minimal predictability of component variation.

In contrast, Maguire (2011:82) provides a more elaborate characterisation of complex systems, which includes attributes such as:

- Numerous elements which interact dynamically;
- Rich interactions where any element can exert and is susceptible to influence from other elements thorough nonlinear, typically short-range interactions;
- The overall system is open, far from equilibrium, and exhibits both positive and negative interaction feedback loops;
- The availability of systemic histories; and,
- Local, component level behaviour is 'ignorant' of the holistic attributes of the system.

While using different lenses of analysis, both descriptions exclude, in principle, highly centralised systems. As a result, the use of complexity as an explanatory paradigm for organisational phenomena must account for the varying role of centralisation in most operational models. At an organisational level, the multitude of employees, vendors, stakeholders, and other third parties which interact to define a company's cyber presence oscillate through a state of critical complexity. However, organisational dynamics are also shaped by top-down interventions, structural systemic constraints, and boundaries in a more

pronounced, scale-specific manner. Thus, the presence of (varied levels of) centralisation in organisations has led to a pluralistic interpretation of 'complexity' in management research: as a metaphor, an analogue, and a true descriptor of social systems (Merali and Allen 2011). This classification is partly philosophically driven. Within the current context, complexity is deemed as a true yet inherently incomplete descriptor of a series of ontological mechanisms which underpin the ontology and dynamics of organisational cyber risk problems (a line of reasoning further elaborated in the Research Philosophy).

Furthermore, within the context of cybersecurity events/cyber risk problems, systemic centralisation is a function of defined scale and locality — concepts which are at least partly eroded by the parameters of cyberspace as a domain of interaction. So, while organisational systems can indeed respond to centralised influences, by incorporating technological interdependencies with highly networked, nonlinear interactions, and an overarching sensitivity to feedback loops, the applicability of complexity as a lens of analysis is consolidated. Particularly within a cybersecurity narrative, the extent of centralisation is diminished by the inclusion of threat interactions and attack surface dynamics which are not a product of (the same) centralised efforts. It is worth noting that exceptions to this line of reasoning can be found for organisations which, either due to their scale or non-reliance on complex and networked information system architectures, exhibit predictable cybersecurity patterns that are a product of centralised characteristics and behaviours. Nonetheless, such organisational examples are not at the core of the cybersecurity debate, given the current state and direction of economic activity highlighted in the previous section on macro-tendencies and cybersecurity. Instead, the increasing reliance on the cyber domain, through its effects on interconnectivity and potential interactions, serves as an amplifier of complexity, non-locality and non-linearity in organisational dynamics.

At a domain-level, Phister (2010) classifies cyberspace as a Complex Adaptive System (CAS) and, in this context, defines the 'adaptive' component as the system's tendency to change its structure and behaviour over time in ways which tend to improve its success. As a result, the term is often equated to an open, dynamic system's sustained existence and growth. The author proposes a number of conceptual implications for cyberspace based on this classification, which include the applicability of the ideas of success and failure (fitness)

criteria, the existence of an internal source of variation, a selection process usable to retain/discard variations which have an effect on fitness, a performance evaluation mechanism, and over-time accumulation and internalisation of variations which maximise environmental fit. In turn, the success of the interacting components of the system (i.e. organisations) lies in their ability to adapt to the dynamics and pressures of the wider context. So, when coupled with the low predictability of system component variation, adaptation becomes a primary mechanism for the pursuit of fitness in Complex Adaptive Systems, and, thus, in cyberspace. (Lansing 2003)

A different perspective on the highly networked interactions and the diffusion/non-locality of cybersecurity phenomena, is provided by Moore (2010) from a cyber economics perspective, through the notion of externalities. More specifically, this is achieved by illustrating three of the types of externalities which can occur: network externalities, which are used to explain the incentives behind the tendency of developers and vendors to prioritise market dominance rather than platform security, and why more secure new products often fail to gain momentum; externalities of insecurity, which can be observed through the variety of losses that are incurred due to a compromised unit (i.e. loss of consumer confidence, market value, intellectual property, opportunities, and other societal costs); and security interdependence, which can encourage 'free-riding', especially in circumstances where overall security depends on the weakest link. In spite of their different disciplinary grounding, externalities are a conceptualisation of the implications which emerge from interactions within complex systems, and encompass co-evolutionary behaviour, emergence, and nonlinearity. (Anderson and Moore 2007)

2.1.5.4 Converging Mechanisms: Non-linearity in Organisational Systems

The ubiquity of nonlinearity and its central role in understanding systems is highlighted by Lansing (2003). Due to its wide applicability, the meta-disciplinary explanatory potential of complexity theory has gained support in a variety of disciplines (i.e. Holling 2001, McKelvey 2001, Folke 2006, Mason 2007, Allen and Boulton. 2011). However, it is important to distinguish between its explanatory and its prescriptive function for the current line of enquiry — cybersecurity as a knowledge problem, resulting in a context-construct gap. The

former consists of attempts to identify ontological mechanisms, systemic ontological demi-regularities and patterns, as well as their characteristics. In contrast, the latter entails consideration for the social component of behaviour, cognition and its sub-constructs, such as time, available resources, and priorities of organisations as an application setting. Given the pragmatic, decision-making context of the problem, the two vectors of analysis must be reconciled in order to gain a flexible, phenomenon-based perspective as a point of departure for prescriptive outputs. On this point, Mousavi and Gigerenzer (2014:1674) note:

"According to the ecological rationality framework, the knowledge of how people should make decisions cannot be studied without considering how people are able to make decisions." (Mousavi and Gigerenzer 2014:1674)

Thus, a sole focus on systemic behaviours can neglect the social parameters of both the problem, and its application setting. In contrast, a purely social perspective of the problem would be insufficient to tackle the complex dynamics exhibited by cybersecurity in organisations. By exploring these two dimensions, the mechanisms they exhibit within the context of organisational cybersecurity can be identified and used to design a conceptual framework which tackles the context-construct gap, and an empirical research strategy. The resulting outputs serve as a foundation for the conceptualisation of a theoretical construct able to facilitate emergence and adaptation/evolution within an organisation's response to cyber risk, while acknowledging the implications — both systemic (Holling 2001) and cognitive (Heuer 1999) — of the application setting's behavioural tendencies. The theoretical utility of such a construct/approach is unlikely to be local, as the core limitations faced by traditional applications of risk management within organisational cybersecurity are the result of emergence from market/system level properties (i.e. externalities, incentive misalignments, asymmetric information, capability gaps and propensity for bias), while the influence of non-linearity on the uncertainty faced within (holistic) organisational cybersecurity is axiomatic. As a result, the following chapters include a review of existing literature covering the systemic complexity, and the behavioural-cognitive dimensions of the cybersecurity knowledge problem.

2.2 Ontological Mechanisms: Systemic Complexity and Hierarchy

2.2.1 Complexity, Metaphors and Mechanisms

The use of systems and complexity theory to frame the knowledge-problem narrative provides a primary ontological foundation for the exploration of organisational cybersecurity as a phenomenon — a pre-requisite for the trans-disciplinary conceptual framework design. The previous section highlighted how systemic complexity is present to varying degrees throughout the cybersecurity context, in spite of the often implicit assumptions of defence paradigms which employ foresight and predictive heuristics. More specifically, a complexity based critical lens of analysis shapes the narrative on key issues such as the nature of the organisational cybersecurity management environment, scale of abstraction adequacy, causalities, dynamism, and linearity, which underpin traditional risk thinking. Ensuring mechanism-based assumptions in the implicit models of the organisational cybersecurity context dynamics allows for the design of a conceptual framework upon which pragmatic constructs, procedures, and action plans can be formulated. (Merali and Allen 2011)

In other words, attempts to solve 'real-world' problems are constrained in their effectiveness by the adequacy of their assumptions concerning the problems themselves (ontological adequacy) and by the contextual efficacy of the methods of choice (analytical adequacy) (Henrickson and McKelvey 2002). The following sections will explore how such constrains can be minimised through an overview of the wider systems theory literature base from the perspective of mechanisms, and will provide a critical outline of the ontological implications these carry for the cybersecurity management knowledge-problem. This will primarily revolve around conceptualising cross-scale open system context (or lack-thereof), order and emergence manifesting (demi-)regularities, and adaptation as a central systemic mechanism in dynamic contexts.

2.2.2 Deconstructing Organisational Systems: Adaptive Cycles and the Panarchy

A core premise of complexity theory is that the degree of system complexity is a

determinant of both the ability and feasibility of understanding its localised dynamics (Lansing 2003, Gershenson 2013). As previously highlighted, through non-linearity, complex systems can amplify small deviations and exogenous stimuli in unpredictable ways (Benbya and McKelvey 2006a). Given that most real-world complex systems are nested, context dependent, continuously interacting and evolving, such deviations are both ubiquitous and instrumental in shaping the patterns under which both organisations and society as a whole operate. In fact, the nested nature of organisations within wider social structures is an expression of the systemic tendency for cross-scale integration.

Within complex systems, elements which interact at similar speeds and spatial attributes can create semi-autonomous levels, each sharing information and materials with the next (Holling 2001, Allen et al. 2014). These multi-level dimensions form "hierarchies" ("hierarchic systems") — a concept that was coined by Simon (1962), who presents them as a frequently occurring structural pattern which enables faster evolution when compared to non-hierarchies. Hierarchies also present distinguishable interactions, both between and within subsystems, thus enabling the analysis of their dynamics. Social systems such as organisations fit a hierarchical structure, encompassing a multitude of substrata which are supported through exchanges of information and materials. At the same time, organisations are subsystems supported by larger levels/structures, such as markets, and are subjected to similar exchanges. From this perspective, cybersecurity processes are nested in an organisational setting both structurally and functionally.

Holling (2001) argues that each level of a dynamic hierarchy has two roles: to conserve and stabilise smaller, faster levels, and to develop and evaluate innovations through same-level experimentation. By containing the variation required to generate innovations within individual subsystems and preserving the fundamental exchanges between the various levels, the integrity of the hierarchy can be supported. Subsequently, altering the properties of the exchanges that take place between the levels of a hierarchy can result in its collapse and reconfiguration. The dynamic, innovation oriented function of hierarchies is represented within the Adaptive Cycle model, which proposes that the future states of a system are a product of three core properties: its change potential, or "wealth"; its controllability, as determined by the extent of the connectedness between the control processes and variables;

and, its adaptive capacity, presented within the model as the antithesis of vulnerability (Holling 2001:394). (Allen *et al.* 2014)

While all three properties seem desirable, the Adaptive Cycle model proposes that complex systems typically navigate a cyclical trajectory consisting of four stages which alter the configuration of wealth, connectedness and adaptive capacity. Given its key role in survival, the tendency to behave in ways which increase potential is an evolutionary imperative for all open systems ('object/structure necessity' Easton 2010). Without potential, they lack both controllability and adaptive capacity, and are thus unlikely to be competitive in acquiring capital, instead being completely dependent on the inertia that is determined by higher levels. Thus, the slow accumulation of capital initiates the adaptive cycle and gradually increases the available potential for both existing and transformed states (exploitation stage). As capital is accumulated, it becomes tightly bound to the processes and variables of the existing system state, and increase system rigidity (conservation stage). The degradation in controllability makes the system vulnerable to "agents of disturbance" who can trigger a rapid release of the accumulated potential (release stage). As the rigid structures are lost in the release process, and the wealth is made available in the ecosystem, it generates new, potentially innovative combinations (reorganisation stage) which form the basis of the subsequent exploitation stage. Unlike the exploitation and conservation components of the cycle, the release and reorganisation are presented as highly unpredictable in both timing and results. The continuous, multi-scale nature of Adaptive Cycles is captured within the notion of a "Panarchy". (Holling 2001, Walker et al. 2006, Allen et al. 2014)

Holling (2001:401) argues that, in human systems, the performance of Panarchies is amplified by three factors: foresight and intentionality, which can mitigate the extreme outcome potential of cycles, but can be hijacked in the interest of subsystems (i.e. individuals), and can be of limited efficacy, particularly in highly complex settings; communication, which enables more efficient coordination between levels and can generate slow moving levels in the Panarchy such as culture and mythology, which affect intentionality (Tansey and O'Riordan 1999); and technology — a scale amplification mechanism that is unique to social systems. By leveraging these factors, organisations influence their navigation of adaptive cycles, through evolving representations of slower-level conditions, same level

innovation potential and presence of agents of disturbance, and faster-level tendencies. At each level, objects and structures compete in reconciling their necessity with the adaptive pressures imposed by wider-level context, creating a network of interdependence. In social systems, this amplifies the importance of adaptive representational efficacy, as positive feedback and pluralistic adaptive drivers are moderated by foresight and intent, communication, and technology.

In spite of their sustaining properties, Panarchies are susceptible to collapse when triggers in the form of a crisis at a smaller, faster level coincide with the release stage of a larger, slower level (Holling 2001). If distinguishing the organisational cyber systems as a level within a hierarchy, the impact of a crisis can transcend its localised nature and reach both slower and faster levels. While it is more likely to affect its sub-levels which depend on it for stability and innovation, it can also trigger the release stage within larger levels, such as the organisation itself. Thus, the impact of sub-system failure on larger, slower levels of the Panarchy is influenced by the continuous dynamic of the Adaptive Cycle. Similarly, the release stage at a cyber systems level can be influenced by triggers from lower levels (i.e. single system component). Establishing subsystem-level foresight requires an understanding of the wealth, rigidity and adaptive capacity of not only the level itself but also of its hierarchical setting of influence. This enables the pursuit of a strategy that is anchored in the dynamics of the setting. Absent consideration for the setting of a specific system and of the properties of its hierarchical dependencies, analytically adequate analysis can yield ontologically inadequate inferences concerning both the probability and the impact of a disturbance.

When used as an ontological heuristic for framing the cross-scale setting of the knowledge problem narrative, the 'Panarchy' construct provides a series of benefits. These include its trans-disciplinary explanatory potential, its compatibility with multi-granular complex system analysis, its spatiotemporal dimension as a source of context specificity, and its emphasis on adaptation and innovation as systemic, multi-dimensional constructs. However, it also provides a number of potential limitations. Firstly, its general explanatory power is contrasted with a limited predictive power — a point of contention affecting complexity studies as a whole (Lansing 2003:200). To address this, the prediction-adverse foundation of complexity thinking is complemented with an emphasis on adaptation which aims to provide an

alternative that strengthens its prescriptive utility (Gershenson 2013). Secondly, agent behaviour-driven variability can alter the apparent sequence progression of the adaptive cycles to an unclear extent. In spite of it being accounted for, the nature, scope and implications of rationality-induced variability in system behaviour can exceed the boundaries of the construct. This is addressed within the following sub-chapter (2.3) of the literature review, in an attempt to incorporate necessary behavioural/'rationality' constructs within the conceptual framework. Finally, describing the dynamic structure of a Panarchy entails a grounding in systemic order and emergence, both concepts discussed at length in the following.

2.2.3 Order and Emergence

Given the reliance of adaptive agents (within the organisational cybersecurity narrative) on schema-based context navigation strategies, both the existence and accurate perception of patterns and distinguishable properties in systemic states — i.e. systemic order — are paramount for adaptive success (Maguire 2011). As an exception, a chaotic state indicates system behaviour that is seemingly random (Levy 1994) and, thus, severely affects the scope of foresight and intentionality. Nonetheless, outside of chaos, non-linear agent interactions lead to the creation of distinguishable — "emergent" — system properties which cannot be inferred based on the mechanistic decomposition of the system into its parts. The notion of emergence was coined in a systemic context to describe properties rooted in scale-specific complexity within hierarchies (Merali and Allen 2011). Such properties are an expression of the interaction patterns between components, the system, and the environment. As such, they can be "multiply realisable", i.e. can be achieved in a plurality of ways (Rickles et al. 2007, Merali and Allen 2011). (Goldstein 2011)

From a cross-disciplinary perspective, Goldstein (2011:66) presents a shared narrative of emergent phenomena, which includes characteristics like: novelty in properties and entities at a macro-level in relation to their micro-levels; unpredictability and "non-deducibility"; macro-level "integrated coordination"; and dynamism. The nature of emergent properties is also influenced by the characteristics of the system. From this perspective, McKelvey

(2001:149) defines organisations as: “quasi-natural phenomena, caused by both the conscious intentionality of those holding formal office (rational systems behaviour) and naturally occurring structure and process emerging as a result of co-evolving individual employee behaviours in a selectionist context (natural and open systems behaviour)”. An alternative view of emergent order which reconciles its self-organisational and constructional dimensions (typical of organisational systems) is provided by Goldstein (2011:73), who proposes “emergence as self-transcending construction”. In such settings, the principles of self-organisation and emergence account for intent, and reflect the interaction between conscious efforts and ‘natural’ structures and phenomena. The prominent significance of scale in conceptualising emergence is of note when considering the effects of intentionality and locality of foresight. At a macro-level in complex, open systems, component-agent interactions can lead to self-organisation, order, and behaviours that are scale-specific, non-mechanistic, and unforeseen at lower, faster levels.

Rickles et al. (2007) emphasise the fundamental role of emergent properties in the formation of hierarchies, as each level affects the next. If viewing the cybersecurity function beyond its engineering/linear systems level, its effects on the dynamics of organisational properties such as vulnerability and adaptivity can be similarly seen as emergent, multiply realisable and non-mechanistic. Attacker access to specific assets can generally be obtained in a plurality of ways, with similar effect for the organisation. Retrospective analysis can provide insight into the nature of a breach, including the establishment of a causal narrative, however its accurate prediction can be unlikely, due to the vast potential spectrum of unknown variables and circumstantial behaviour. Even retrospection can fail at times to generate insight with a high level of confidence, as illustrated by the difficulties of attribution for specific cyber-attacks (Rid and Buchanan 2014). This is amplified by the direct effects of potential prediction on the narrative itself: foreseeing and addressing a specific threat-vulnerability tuple which would have otherwise led to a breach can either deviate the narrative, pushing the organisation, as a multi-stable system, towards an alternative evolutionary path, or potentially lead to the same result depending on threat behaviour, alternative vulnerabilities, and other unforeseeable factors.

However, Lansing (2003:185) highlights how patterns of emergence often become

apparent, despite the 'unsolvable' causalities which shape the behaviour of systems exhibiting nonlinear dynamics. Such patterns are pivotal for the rational interpretation of complex system behaviour, and can provide actionable insight concerning problems which are not decomposable. Due to the coevolutionary relationships shaping levels within hierarchies, distinguishable patterns of system or agent behaviour are the foundation of rational feedback and, implicitly, foresight and intentionality, communication, and technology (Holling 2001). For example, in spite of variation in both the behaviour and consistency of its individual members, the culture of organisations is generally stable and cohesive (Miller and Page 2007). Conversely, from an organisational perspective, Smith (2003:252) finds that "… culture change is one of the most difficult types of change to accomplish". Authors like Thomson et al. (2006) have called for the "cultivation" of an IS culture as a way to address 'the human component' of vulnerability. However, even if assuming the human component to be a cohesive, distinguishable dimension of IS, proposals of culture design neglect its emergent nature. As a higher level of the organisational hierarchy, the functional role of culture is stability inducing, enabling the cohabitation and coordination of lower, faster levels. In the absence of pressure from even higher-levels, i.e. business environment, intentionally altering culture dynamics based on a hypothesised causal logic can prove to be maladaptive, leading to unintended consequences. This is supported by the findings of Harris and Ogbona (2002:47) who have found the unintended effects of top-down culture change efforts to be both "pervasive and profound".

Nonetheless, emergent patterns lie at the foundation of feedback and foresight within complex settings. Their probabilistic consistency is essential for effective planning, forecasting and analysis. However, the previously highlighted implications of multi-directional causalities and non-linearity as limitations in mechanistic (and even non-mechanistic) prediction also outline its boundaries and variable efficacy. It should also be noted that, despite the incommensurable range of potential interactions which can occur in a Panarchy, the range of total potential outcomes can be differentiated from the range of plausible outcomes. Predictive efforts within such settings are not all equivalent, and can be manifested in a range of initiatives: identifying predispositions at a specific level of a hierarchy within adequately chosen spatial and temporal parameters can seem significantly more likely to yield results than mechanistic forecasts. Even so, intentional attempts to alter emergent properties in

anticipation of perturbations and stress should acknowledge both the potential and the epistemic limitations of such efforts, especially if these rely on inference and extrapolation from level-specific indicators, as hierarchical system levels themselves often fail to align in predictable ways (Benbya and McKelvey 2006b).

In line with Holling's (2001) viewpoint, the co-evolutionary properties of hierarchies, manifested through the continuous nature of emergent parameters which shape fitness pressures, lead to the formation and destruction of competing structures for capital extraction and use. This phenomenon is at the core of conceptualising cyber resilience: if viewing cybersecurity as a dimension of an organisational hierarchy, environmental fitness pressures are buffered by rational structures which prioritise the hierarchy's main goal: sustained performance in wealth extraction. Due to their hierarchical context, the fitness parameters of cyber systems are imposed and supported by the organisation, rather than the wider environment. As wealthy systems are able to pursue a wider range of potential states, wealth extraction effectiveness can lead to a potential disconnect between the wider fitness pressures imposed by the environment on an organisation, and their rational interpretation and implementation in lower levels. So, as a nested system, the ability of perturbations within cyber systems to be supported by their organisational setting is inversely proportional with rigidity of the organisation itself: if it doesn't trigger the release stage, the wider level can support and alter the lower levels.

To summarise, a hierarchical and continuous view of complex systems can be used to explain the key ontological dynamics which underpin the cybersecurity management knowledge problem. Patterns within emergent properties are an essential source of foresight and feedback, however, even if accurately identified, their non-mechanistic nature makes their conversion into action dependent on heuristic assumptions rather than absolute relationships. The continuous spatiotemporal nature of intra and inter level dynamics is reflected in multiply-realisable emergent properties such as vulnerability and adaptive capacity, while foresight and intentionality, as well as exogenous pressures and triggers, can shape the trajectory of the system/organisation between different states of stability.

Based on this framing, the likelihood of a cyber incident triggering a release stage at an

organisational level is dependent on the overall state of the organisation. Highly stable environments with sufficient adaptivity and wealth are able to maintain their integrity even after significant perturbations, whereas highly rigid or poor (lacking wealth) systems are inherently more vulnerable. Even in circumstances of vulnerability, the systemic collapse of an organisation can also be prevented by mechanisms and events in higher, stability inducing, societal level. This explains why, despite the significant and varied costs incurred by companies due to cyber incidents (Thomas *et al.* 2013), these do not regularly undergo large scale visible release stages. While the cyber-layer of organisations has shown exploited key vulnerabilities, the wealth, higher layers' resilience and external support mechanisms have prevented their systemic unravelling. However, as the aggregate non-local effects of such incidents can shape the stability, dynamics and fitness pressures of the emerging security climate, the local avoidance of rigidity, low resilience, and competitive disadvantages relies on the use of adaptation as an evolutionary mechanism.

2.2.4 Evolution, Adaptation and Exaptation

"Adaptation at the macro level (the 'whole' system) is characterized by emergence and self-organization based on the local adaptive behaviour of the system's constituents. "(Merali and Allen 2011:41)

The adaptation to, and navigation of complex, highly dynamic environments without schema-based rationality is arguably the norm for most open systems. Evolution, as a construct, conceptualises the mechanism which underpins blind adaptation and drives emergent structures/forms over spatiotemporal contexts. Beinhocker (2007:214) outlines evolution as a substrate-neutral, recursive "algorithmic process of variation, selection, and replication…" undergone by interacting agents, based on fitness constraints imposed by their environment. Subsequently, it addresses a dynamic search problem — finding and shaping suitable system parameters which enable adaptation — and demonstrates distinct effectiveness at balancing the exploration and exploitation of an environment. Interdependence also plays a significant role in evolution, as highlighted by Benbya and McKelvey (2006b:287) ("all 'evolution' is really coevolution…"). The following section will

address the notion of adaptation as both an emergent process, and as the product of intentionality.

Garud et al. (2016:150) present the term “Adaptation” from an evolutionary biology perspective, in its noun form, as an “Aptation” — which is succinctly defined as “being fit” — containing a characteristic that results from natural selection for its current role. Thus, the adaptation process entails the development of such characteristics based on subjection to fitness pressures. In contrast, the term “Exaptation” describes a fitness improving characteristic which has emerged through natural selection for the fulfilment of a different use (Garud et al. 2016). The latter was introduced by Gould and Vrba (1982), who found that the use of adaptation as a blanket term for fitness enhancing features distorts the historical origin of said features, and fails to distinguish between their function (evolutionary role) and effect (the current usage). Larson et al. (2013) highlight how Gould and Vrba’s (1982) proposal has failed to gain traction within evolutionary biology, likely due to its limited differentiability from adaptation, given dynamic multiple selective pressures and the incremental nature of evolution: most existing features have evolved from previous iterations under which they are likely to have had a different effect (Larson et al. 2013).

However, outside of evolutionary biology, where selection is a 'blind' process, the notion of exaptation has met significantly more success (Larson et al. 2013). In contrast, foresight, or guided variation, enables the clear identification of purpose thus facilitating the differentiation between (teleological) function and effect. This differentiation is particularly important within the context of disciplines which place an emphasis on the intersection of variation and foresight, such as innovation studies (Bonifati 2013, Garud et al. 2016) and evolutionary economics (Gowdy 1992, Dew and Sarasvathy 2016). The redeployment of existing resources to a different effect in response to changes in the environment is also represented in strategic management theory in the form of the “dynamic capabilities” construct (Teece et al. 1997, Eisenhardt and Martin 2000). As the latter has evolved from a different, semi-independent body of literature, it can be seen as an indicator of explanatory pressures within the organisational management literature concerning the importance and means of enabling (ad)aptations and maximising adaptivity through foresight.

It is important to note that the presence of foresight is not an absolute determinant of exaptation. Guided variation can be complemented by "stochastic forces" (i.e. learning errors) and ecological adaptation (Larson et al. 2013:497). Furthermore, interacting agents with intentionality can collectively exhibit ecological properties — a core premise of the Complex Adaptive Systems perspective (Lansing 2003). Miller and Page (2009) emphasise the tendency of social agents to form connections, which lead to nonlinear interactions and the formation of complex systems used for the navigation of adaptive processes. It is also highlighted that change (variation) can be pursued by individuals through deliberations about the environment, which may result from either direct cognition, or from potentially mutable "stored heuristics" (Miller and Page 2009:10). The authors also illustrate emergent patterns of consistency and cohesion which characterise the dynamics of social CASs. Thus, coevolutionary pressures are manifested through adaptive and exaptive changes in the nature of the connections, which, in turn, affect the shared deliberations which underpin culture.

According to Benbya and McKelvey (2006b:285), the coevolution between organisational levels and the environment "involves a continuous process of adaptation and learning along with some degree of experimentation". The three factors are interdependent and seemingly generalisable even in 'blind' settings. Holling (2001) presents an intent-agnostic perspective of learning as a result of system change, i.e. transitions between stages within an adaptive cycle. Competing structures at each level of a hierarchy generate variation — analogous to the function of experimentation, while the foundation of the variation process consists of historically fit structures, or their remnants after a release stage. These predispositions are 'blindly' learnt and form the basis for both adaptation and exaptation given the historical path dependence which characterises complex systems (Manson 2001). Through foresight, communication, and technology, rationality entails the availability of a significantly broader epistemic toolbox for the navigation of coevolutionary, adaptive pressures. As a result, targeted variation can decrease the rate of maladaptive properties and maximise the utility of available system wealth, while selection strategies enable the identification of exaptive structures and fitness pre-emption. Finally, through communication and technology, the replication pace and scale of the outputs of selection can be vastly amplified. Subsequently, rationality in systems can be a lever of influence on the adaptive process.

2.2.5 First Principles of Adaptation

As a foundation for the operationalisation of complexity theory, Benbya and McKelvey (2006a, 2006b) propose seven complementary principles of adaptation in social and/or biological systems extracted from an extended theoretical review. These principles are presented as "one logic step above self-evident foundational axioms…" (Benbya and McKelvey 2006a:21), and encompass:

- The adaptive tension principle, whereby the creation of adaptive order is stimulated by environmental tensions in the form of "energy differentials";
- The requisite complexity principle, which entails that the creation of adaptive order depends upon internal complexity exceeding external complexity;
- The change rate principle, asserting that, in dynamic environments, an adaptive advantage is attributable to higher internal change rates;
- The modular design principle, based on the premise that near autonomy in subunits can increase complexity and the adaptive response rate;
- The positive feedback principle, which proposes that seemingly insignificant events amongst agents or modules can lead to order creation;
- The causal intricacy principle, whereby complexity entails dealing with multiple causes ("bottom-up, top-down, horizontal, diagonal, intermittent, and Aristotelian");
- The coordination rhythms principle, built on the premise that alternating rhythmically between sources of causal dominance creates functionally superior adaptive responses than balance. (Benbya and McKelvey 2006a:21)

While non-exhaustive, the seven principles conceptualise a thorough, meta-disciplinary representation of adaptive properties within complex settings. Furthermore, they complement the emerging ontological representation of adaptation as a key determinant of open system 'survival' in dynamic, non-linear settings. Thus, similarly to the Panarchy construct, they serve a heuristic function in conceptualising the knowledge problem narrative. Absent adaptation, the selective pressures generated by the continuously evolving environment can impose a lack of fitness onto the organisational hierarchy, decreasing its competitiveness and sustainability. This inference is built on a conceptualisation of the 'cyber

function' as a manifestation of a system level which can be placed on the spectrum of openness, through what McKelvey (2001:149) describes as "quasi-natural phenomena": a combination of conscious intentionality and naturally occurring emergence.

An alternative perspective consists of decreasing systemic openness by restraining and delimiting an organisation's cyber presence. Closed systems are not susceptible or responsive to external influences, exhibiting exclusively internal dynamics (Rickles et al. 2007). However, this view is contradictory to the fundamentally expansive, interaction-orientation of the cyber domain. Kuehl (2009) argues that cyberspace is not definable solely through electronic infrastructure and physical components, instead comprising of the emergent phenomena enabled by said infrastructure. This perspective is not uncontested. The use of the word 'cyber' itself is frowned upon by many security professionals, being seen as meaningless and overly abstract, while indicating limitations in the operational understanding of its user (Dickson 2015). However, authors such as Kuehl (2009) or Nielsen (2012) do not use the term to substitute operational unfamiliarity. Instead, they use it to describe and contextualise an emergent domain of human endeavour — a holistic view. From this perspective, security proposals to constrict said emergence and pursue a transition towards a more 'closed' system approach is, with few exceptions, counterintuitive and inconsistent with meta-functional adaptive pressures.

In summary, an ontological framing of cybersecurity management based on a complex systems perspective enables the development of holistic and generalisable explanatory framework. It also highlights the limitations of sole reliance on a mechanistic causal narrative, while providing a series of alternative heuristics and concepts, such as Adaptive Cycles, the Panarchy, Emergence, (Co)Evolution, Adaptation and Exaptation. An overview of the fundamental role of rationality, intentionality, foresight, communication and technology has also been presented within the context of non-linear dynamics, further enforcing the 'knowledge-problem' perspective. The following sub-chapter will further explore the social/behavioural mechanisms of reason which influence organisational order creation and underpin organisational cyber risk practice. This exploration enables a critical examination of the nature, extent, and attributes of assumed contextual 'rationality' as a construct in prescriptive organisational cybersecurity management frameworks. In turn, coupled with the

systemic, ontological emphasis on dynamism, complexity, emergence and adaptation, an account of ‘rationality’ provides a bedding for empirical investigation, while also grounding assumptions in a general (epistemic) conceptual model.

2.3 Behavioural Mechanisms: 'Rationality' and Social Adaptation

One of the highlights of the previous section has been that social levels/systems in a Panarchy can coordinate endogenous forces to alter their context and behaviour through their use of schema-based 'rationality' and intent. The ability to manipulate both systemic properties and the evolutionary process is fundamental for human/social endeavours. But a high-level representation of rationality and cognition within the context of what Holling (2001) classifies as the distinguishing traits of human systems: foresight and intentionality, communication, and technology — can prove to be incomplete across levels of analysis.

Assumptions about behavioural/cognitive patterns and mechanisms are embedded within the likelihood evaluation of events which involve – i.e. can be altered by – actors as adaptive agents. Subsequently, this potentially affects both the accuracy and the effectiveness of inferences concerning the role and tendencies of organisational decision-makers who drive cybersecurity policy and strategy, the operational patterns of actors who engage with and rely on the ICT infrastructure to generate value, and the motivations and means of threat actors which introduce the vectors of adaptive pressure. So, as an emerging aspect of the research narrative, the section aims to provide a critical overview of rationality and reasoning as contextual constructs which underpin such behavioural inferences. March (1978:589) argues that rational choice is based on guesses concerning the potential consequences of action, and guesses of preference concerning these consequences. However, the assumption of a cohesive, collectively held view of the choices which shape an organisation's cybersecurity management narrative which maps to an observer-independent reality is implausible within the context of the emerging conceptual framework.

This section will explore the reasoning behind this implausibility, while attempting to establish an alternative, contextually adequate base of assumptions. By doing so, the level of abstraction of constructs such as 'intent' can be decreased, resulting in a more detailed, functionally oriented representation of the nature and effects of adaptive agent behaviour, as applied to decision making within a complex systems context. A critical representation of 'rationality' is also paramount for establishing prescription, given the causal significance of

agent behaviour (variation) in cybersecurity outcomes. Emphasis will be placed on both the role of individual cognition mechanisms and on the influence of social structures for decisions within cybersecurity management, and its associated uncertainty. However, the literature review does not attempt to address cognition and decision making exhaustively — a vast, continuously developing area of academic enquiry. Nor does it aim to provide a rigid, final, or mono-disciplinary outlook of the problem area. Instead, it aims to advance the 'knowledge-problem' framing and guide subsequent outputs by outlining some key considerations for (implicitly) modelling rationality within an organisational cybersecurity setting.

2.3.1 Foresight and Intentionality: Reasoning and Inference Mechanisms

Attempts to mitigate uncertainty, optimise decision making and, thus, address cybersecurity management as a knowledge problem, inherently encompass a cognitive dimension. McKelvey (2001:149) identifies rational order in organisational systems as a result of "prepensive conscious intentionalities". This is in contrast to open and natural systems/order, the former being defined by exogenous forces, with the latter emerging from actor interactions. As composite entities, social systems converge the top-down intent of structurally key individuals who are tasked to represent the necessities of the wider structure, with the bottom-up behavioural dynamics of actors who manifest a heterogenous base of intent. Thus, both top-down and bottom-up dynamics are a function of locally conditioned decision-making and action.

However, modelling and supporting actors as decision makers can be a significant point of contention: assuming varied forms of irrationality — i.e. high behavioural entropy — may prove inefficient, whereas representing actors as homogenous and unboundedly 'rational' (a notion further explored throughout the chapter) may prove unrealistic (Gigerenzer 1996). This problem lies at the bedding of a plethora of social disciplines. For example, Tansey and O'Riordan (1999) contest the use of economic rationalism and the utility principle from the perspective of social risk theory. Sabau (2010:1194) highlights the shortcomings of unrealistic assumptions concerning the boundaries of foresight in constructs such as 'Homo Economicus'. While seemingly preferable over assuming behavioural variability when

modelling an unknown decision maker, such a monolithic approximation of human tendencies, preferences and foresight, absent context significantly limits both the prescriptive and explanatory potential of resulting outputs — a key insight of behavioural economics (Krugman 1998, Thaler 2000, Manson 2001).

The idea of schema-based adaptive agents was introduced in the previous chapter within the context of a systemic account of organisational actors. In this sense, it is used to describe behaviour guided by evolving (representational) models of reality upon which behavioural tendencies and intentionality are predicated. Thus, representational mechanisms are central to constructing 'rationality' which, expanding on March's (1978) description, entails contextually normative guesses of potential and preferred consequences in a given situation. Similarly, Sloman *et al.* (2012) propose a causal model of intentionality judgement which is built on conceptualisations of representations (i.e. behavioural foresight) and meta-representational processes (i.e. awareness). At an individual level, the development of new representations, such as the likely conditional outcomes of a given situation, based on previously held representations, such as beliefs about the nature of the situation, is a function of inference (Mercier and Sperber 2011). However, this process is not inherently conceptual, deliberate or conscious. In contrast, reasoning — a specific form of inference which is archetypically associated with rationality — describes the conceptual process of developing a new representation by consciously considering its previous representations/premises. (Mercier and Sperber 2011)

Given its apparent procedural transparency, its compatibility with representational dissemination/communication, and its potential responsiveness to social moderation, reasoning is functionally linked to rationality through its role in yielding normative contextual representations and manifesting patterns in foresight and intentionality. However, the merits of such reason-based interpretations of rationality are prone to critique based on both descriptive and pragmatic/prescriptive grounds. Descriptively, Sperber and Mercier (2012) present reasoning as a social/argumentative meta-representational function that is distinct from the individual inferential generative mechanisms which drive novel representations. Thus, at a cognitive level, intuitive inferences are opaque to conceptualisation, while reasoning functionally enables social moderation and adaptation in representational models.

In other words, proponents of this 'argumentative view' (Mercier and Sperber 2011) hold reasoning to serve a primarily social meta-representational function that is distinct from individual inferential/representational mechanisms.

Subsequently, the internally opaque nature of (most) individual inferences, and their post-hoc meta-representational construction reaffirm the pragmatic interpretation of 'rationality' — a stance which will be prevalent throughout the remainder of the chapter. As a pragmatic concept, it can be used to describe inferential and behavioural patterns and tendencies, i.e. order, in dynamic environments. However, critical emphasis is placed on the mechanism-derived limitations of rationality (Tversky and Kahneman 1974, Kahneman and Frederick 2002), on the contextually bound merits of 'rational' strategies (i.e. model-based), as opposed to heuristic (Mousavi and Gigerenzer 2014), or adaptive strategies (March 2006). Indeed, the development of pragmatic, mechanism-oriented assumptions for an organisational cybersecurity context must account for rationality in both its individual-cognitive and its social-adaptive dimensions. This division is reflected in the following sub-sections.

2.3.2 Pragmatic Rationality: Heuristics and Biases

The growing body of work addressing the limitations of a monolithic 'rationality' perspective, in its modern form, is traceable to Tversky and Kahneman's (1974) propositions concerning the role of Heuristics and Biases as central mechanisms in decision making under uncertainty. At the core of their original findings is the assertion that in complex, uncertain circumstances, individuals consistently rely on judgmental heuristics which are used to reduce the complexity of the task. In spite of their overall functionality, these heuristic principles can lead to significant "systematic errors" (Tversky and Kahneman 1974:1124). Based on this, Tversky and Kahneman (2002:15) define the notion of a "judgmental heuristic" as "a strategy — whether deliberate or not — that relies on a natural assessment to produce an estimation or a prediction". Thus, the reasoning errors which result from a reliance on cognitive shortcuts are distinguished by their deviation from normative decision-making behaviour, as opposed to the favourableness of the resulting outcomes. More specifically, Kahneman and Frederick (2002) argue that heuristic judgments can be identified through their replacement of a 'target

attribute' of a judgement object with a different, more accessible property of the object — a 'heuristic attribute'. Biases occur when there is a discrepancy between the target and the heuristic attributes, thus misguiding intentionality.

Tversky and Kahneman's (1974) early experiments postulated three heuristics — Representativeness, Availability, and Adjustment and Anchoring — which underpin a variety of cognitive biases: the Representativeness heuristic describes the role of mental construct resemblance on probability assessments; the Availability heuristic indicates a link between the estimated frequency or probability of an event and the ease of its recollection; and the Adjustment and Anchoring heuristic proposes that sequential estimates are influenced by the starting point. In their revision of the original framework, Kahneman and Frederick (2002) argue that Anchoring falls outside of the stated definition of a judgement heuristic, and should instead be replaced with the Affect heuristic, which illustrates the role of the emotions and intuitive reactions ("affect valance") associated with stimuli on decision-making. Slovic et al. (2005) highlight the centrality of Affect for "dual-process theories of information processing". Such theories divide perception and, thus, decision-making into two systems: System 1, predicated on intuition and experience, and System 2 characterizable as analytical and rational. (Evans and Frankish 2009)

The role of Affect in decision making is supported by independent lines of enquiry. Bechara and Damasio (2005:338) illustrate said role through the 'Somatic Marker Hypothesis', which is built on observations of tendencies towards detrimental decision-making exhibited by patients with lesions on their ventromedial prefrontal cortex. The effects of the damage are only manifested through a compromised capacity to adequately express and experience emotions, which, through experimentation, have been argued to lead to limit somatic response intake, and prevent future loss aversion. Based on this, Bechara and Damasio (2005) also argue that, when isolated, conscious knowledge — previously framed within System 2 — is insufficient for making advantageous decisions. The centrality of potentially contradictory interactions between System 1 and System 2 reasoning based on context is also empirically illustrated by Sloman (2002). Furthermore, Kahneman and Frederick (2002) highlight that heuristics are not an inherently System 1 phenomenon; instead, they can be used as a deliberate System 2 strategy.

In spite of the Heuristics and Biases framework's significant impact and volume of follow-up experimentation and analysis, critics have contested both individual results (i.e Koehler 1996, who found the Representativeness derived 'base-rate fallacy', whereby subjects tend to ignore prior probabilities, to be overstated), and the broader approach taken by the authors. Most notably, Gigerenzer (1996) argued against the content-blind Bayesian normative logic used in the original experiments, especially within the context of single-event probabilities. In addition, he suggested that the results could have been conditioned by the experimental design, whereas the models underpinning the framework have limited explanatory power. These points of critique are addressed by Kahneman and Frederick (2002), who suggest that while they are conceptually plausible, they do not account for the consistency in findings achieved by follow-up, varied experiments.

Mousavi and Gigerenzer (2014) outline an alternative view concerning the role of heuristics in addressing uncertainty. They argue that measurable risk is based on two possible types of assessment: 'a priori' probability, which is inferred from the known properties of an application setting, and produces deterministic knowledge; and statistical probability, obtained through data collected from repeated observations within a homogenous setting, resulting in stochastic knowledge. Given the limited applicability of such assessments in many real-world decision-making settings, Mouvasi and Gigerenzer (2014) suggest that action is often derived from estimates. Therefore, in the presence of uncertainty, actions rely on heuristics which are manifested through intuition and 'satisficing' solutions, rather than statistical thinking. Bingham and Eisenhardt (2011:1458) support this view, finding that, in addition to being less effort-intensive than more complex insight generation methods, heuristics can also yield superior foresight in strategic action. The authors also propose that the predominantly negative perspective on heuristics is attributable to the strategically irrelevant, artificial nature of the simulated decision-making environments which form the basis of much of the experimental research conducted within the field.

The ubiquity of heuristics can also be explored in relation to the bound nature of cognition and perception. Within the context of theoretical biology, Mark et al. (2010) propose that human perception has evolved to discern an incomplete, estimated representation of an

observer independent reality. This is due to the fact that, from an evolutionary perspective, given equal resources, models of perception that are functionally fit and represent approximations of relevant occurrences outperform 'naive realist' models, under which perception "exhaustively resembles reality" (Mark et al. 2010:505). Thus, selective perception, as opposed to broader/more accurate alternatives, can prove to be a superior perceptual strategy. In this sentiment, Gigerenzer and Brighton (2009) argue against the "accuracy-effort trade-off", which they present as a theme of the Heuristics and Biases literature, built on the premise of a positive causal relationship between the amount of cognitive effort invested and accuracy of subsequent results. Furthermore, they argue that heuristics are neither inherently good nor bad; instead, they rely on contextual fitness ("ecological rationality") for generating adequate results. In turn, this is not reflected through a single measure, but by a learning curve which considers the effect of accumulating observations on bias and variation. This assertion is contrasted with Tversky and Kahneman's (1974) approach of evaluating the presence of sub-optimal decision-making as a measure of deviation from a normative process rather than a specific result.

Gigerenzer and Brighton (2009:128) present three underpinning components of heuristics: search rules, which set the criteria for the exploration of cues; stopping rules, which indicate that sufficient cues have been explored; and decision rules, which lead to the selection of a course of action. Through permutations of these three components — coined 'the adaptive toolbox' — a wide variety of heuristics can be generated. The selection of a heuristic is proposed to depend on at least three principles: memory, feedback/reinforcement, and environmental structure (Gigerenzer and Brighton 2009). It is worth noting that this approach towards heuristics does not negate the link between System 1 representations and biases. Instead, it highlights that solely associating heuristics with biases paints an incomplete picture of their potential utility, and unavoidable role in circumstances where System 2 cognition is constrained, such as cognitive overload (Pfleeger and Caputo 2012), or unfeasible.

Thus, heuristics can be explored through the ontological, complexity oriented constructs covered in the previous section as adaptive mechanisms used for exploring indicators of emergence while ignoring micro-causal information. When used within an appropriate setting, they have been argued to potentially yield better results than more complex

competing models (Gigerenzer and Brighton 2009, Brighton and Gigerenzer 2015), especially as they show adaptation based on accumulating observations. While seemingly optional as a System 2 strategy, heuristics are fundamental for System 1 decision making, playing a key role in foresight and intent, especially under uncertainty or when faced with conditions which impede on the reliability of System 2 thinking. However, the limitations of heuristics are also reflective of boundaries in individual cognition. They can result in biases which impede perceptual adaptation, thus generating a disconnect between intent and outcome. This is particularly distinguishable within the context of affect as a determinant of System 1 cognition. Given its externally opaque nature, the influence of individual affect can be difficult to gauge, which can lead to incongruity between explicit analysis and intuition, especially within collective settings. When conditioned by previous experiences that are anomalous, unrelated or non-generalisable, intuition can lead to myopic assessments of consequences, or unjustified levels of confidence. In contrast, affective insight can result in advantageous courses of action, even in complex or uncertain settings given contextual fit.

So, when modelling individual intent and foresight within the context of cybersecurity management assumptions of omniscience, or even perceptual objectivity are unfounded. Gigerenzer and Brighton's (2009) adaptive toolbox emphasises the role of heuristic learning through repeated interactions with a homogenous and repeatable problem in order to achieve ecological rationality. However, cybersecurity presents numerous instances of single, as opposed to repeated events, with varied affective impact: in complex social structures such as organisations, the individual affective perception of a systemic disruption is neither homogenous nor general. Such circumstances can impede on the potential of heuristic adaptation and learning in balancing foresight and intent.

Tversky and Kahneman's (1974) findings show numerous potential misapplications of the heuristic mechanisms that shape foresight, which include unjustified confidence in both predictions and instance predictability, as well as unawareness of perceptual limitations (Gilovich et al. 2002). These findings reflect that of Heuer (1999) within the context of intelligence development, and Pfleeger and Caputo (2012) within cybersecurity. Another issue within cybersecurity management foresight is that of feedback. As strategic success is indicated by the absence of an actively exploited Threat-Vulnerability tuple, threat behaviour

is a key determinant of success, yet is often opaque and exogenous, potentially leading to misleading assumptions concerning the effectiveness of decision making. Generally ineffective strategies can be pursued without detrimental consequences absent threat activity, whereas broadly effective strategies may fail to prevent low probability or high threat capability breaches. Thus the distinct nature of the problem can affect the efficacy of System 1 adaptive mechanisms. Finally, while dual-process theories position individual decision making at the intersection of System 1 and System 2 thinking, the quintessential role of social structures, communication and coordination across social systemic hierarchies must also be noted. Furthermore, communication and coordination mechanisms condition the ability of individuals to project, shape, and adapt intent at a systemic level — all key aspects of conceptualising the organisational cybersecurity context-construct gap.

2.3.3 Social Adaptation: Communication and Coordinated Representational Structures

At a finer level of conceptual granularity, McKelvey's (2001) previously quoted description of rational order in organisational systems entails the interaction of individual-actor mental models, which shape perception and estimates of consequences and preferences (March 1978), with social models encompassing (social) norms, roles and meaning (Sunstein 1996). Norms are defined by Sunstein (1996:11) as "social attitudes of approval and disapproval"; 'roles' are presented as social divisions associated with networks of appropriate norms, and 'meaning' is used to describe "the expressive dimension of conduct" which "involves the attitudes and commitments that the conduct signals" (Sunstein 1996:19). These constructs, are used as building blocks for an outline of the social/collective dimension of influence over conduct and decision making — an extension of the individual perspective. It is worth highlighting that, through its cognitive nature, decision-making is individual-bound. However, as illustrated by Sunstein (1996), given the role of social structures on the context of individuality and conduct, these are analytically inseparable when attempting to explore the behavioural mechanisms at play in organisational cybersecurity management.

Matsumoto (2007:1286) proposes individual behaviour to be "the product of the interaction

between culturally dependent social roles and individually different role identities". As such, he outlines cultures as emergent constructs shaped by the interaction between the problems faced within an ecological context, which take the form of "biological needs and social motives", and the approaches used by a group to solve them, which are constrained by the available resources. The resulting solutions — "environmental adaptations" — drive culture dynamics (Matsumoto 2007:1291). This perspective touches upon a series of themes: the contextual dependence of culture, norms and meaning; the role of culture in disseminating adaptive behaviour which enables biological and social problems to be solved; and the specificity of the configurations of social collectives and constraints in relation to specific environmental adaptations. Singelis and Brown (1995) also highlight the self-perpetuity of culture, the mix of physical and aggregated mental construction ('subjective culture') of its members, the two-way hierarchical nature (i.e it supports the lower levels which, in turn, underpin its dynamics), and individual-bound manifestation (its effects are observable within the behaviour of individuals).

Thus, using Holing's (2001) characterisation of social systems, culture serves a communication function that is manifested through both implicit and explicit exchanges. More specifically, implicit communication occurs in the form of interaction between actors and groups which share norms and meaning, coordinate in hierarchies beyond the constraints of direct interaction, and possess individual roles and shared objectives in the form of social and ecological imperatives. Furthermore, it serves as a platform for the identification of environmental adaptations, and their dissemination through adaptive pressures and explicit communication (Matsumoto 2007). Snowden (2002:103) explores the duality of culture as a catalyst for knowledge which is manifested as both a measurable, observable "pattern of residence and resource exploitation", and as an "ideational system" embodying the less tangible implicit communication functions through shared ideas, conceptual systems and norms.

But the delimitation of cultural homogeneity must also be taken into consideration. For example, Clarke (1988) finds that, within the context of risk analyses, their unavoidably social nature is also a source of potential distortion and biases of a political nature. As the analysis, decision making and implementation of a risk based policy often involves different actor

clusters (with different roles and norms), whose views must converge on a simplified outlook of a problem and its implications, structural influence imbalances can significantly shape the outcomes and impose ideological bias. Unlike intentional deception, Clarke (1988:161) positions ideological bias as a function of the "ontological assumptions that underlie an actor's world-view" — which is consistent with Kahneman and Frederick's (2002) outline of the construct. Thus, the power division of an organisation can deviate the contextual ecology of risk assessments, or other similar System 2 heuristics. Role-based structural divisions also incentivise the emergence of subcultures with distinguishable norms, adaptive pressures, affective contexts, and degree of influence over decision-making. Such divisions are likely to internally promulgate ontological assumptions as per Snowden's (2002) assertions, which affects the ways in which adaptive feedback is internalised.

Within the context of cybersecurity management, Pfleeger and Caputo (2012) found several decision-making cognitive limitations which illustrate the core points of the discussion so far. These include: the framing of security thinking as a secondary function; the detrimental effects of cognitive overload over the process of analysis, which also illustrates the limitations of System 1 thinking in security risk scenarios; the presence of inattentional blindness (failure to notice unexpected occurrences while focusing on a primary task); significant bias rooted in previous "experience, goals and expertise" (Pfleeger and Caputo 2012:602), which reflects Clarke's (1988) narrative concerning ontological assumption variation within stakeholder groups, and, thus the political dimension of risk analysis; and the significance of perceptual limitations within time constraints.

The social moderation of ontological assumptions is also dependent on externalised, i.e. trans-personal, inference procedure formalisation. In this context, Heuer (1999) explored cognitive limitations as part of intelligence analysis, concluding that, within instances of uncertainty (natural, or induced) and complexity, a reliance on implicit psychological mechanisms of orientation and decision making often leads to biases and low analytical efficacy. While not fully avoidable, he argues that the effects of such limitations can be mitigated through explicit tools and techniques which promote critical thinking in relation to assumptions, illustrate the extent of the uncertainty faced, and encourage the development of alternative points of view. These assertions do not conflict with Gigerenzer and Brighton's

(2009) insight concerning the positive potential of heuristics and of the adaptive toolbox. Instead, they are based on the idea that, by externalising the adaptive process within a multi-stakeholder setting, a broader contextual ecology can be pursued, reconciling the potentially pluralistic drives of sub-cultures. A critical, diverse base of adaptive feedback concerning the ontological assumptions which underpin organisational decision-making is more likely to perceive and correct inappropriate uses of heuristic attributes, from the perspective of different norms, roles, and meanings. Heuer (1999) argues that, for such a structure to be achievable, an explicit process of rational analysis that adequately employs tools and procedures for the development of a collective, transparent, and non-localised (interdisciplinary/ interdepartmental) perspective.

To summarise, there is a growing body of literature exploring the descriptive tendencies and mechanisms shaping the pragmatic boundaries of rationality as a construct. Inconsistencies in decision making under uncertainty can emerge from perceptual approximations and cognitive shortcuts in the form of implicit heuristics, affective context and foresight, informational availability and format, cognitive capacity and availability, social structures and culture manifested through roles, norms and meanings, as well as personal goals, capabilities and available tools. While pragmatically unavoidable, and even potentially beneficial, as demonstrated by the potential effectiveness of Heuristics (Gigerenzer and Brighton 2009, Bingham and Eisenhardt 2011, Mousavi and Gigerenzer 2014, Brighton and Gigerenzer 2015), or by the evolutionary success of incomplete perceptual strategies (Mark et al. 2010), such mechanisms can also generate significant representational deviation and lead to contextually inadequate strategies (Heuer 1999, Pfleeger and Caputo 2012).

The tendency for representational deviation can also affect the communication of analytical outputs, due to the numerous mechanisms which shape their interpretation. Kahneman and Frederick (2002) propose that bias mitigation can be encouraged through System 2 reasoning. So, in joint stakeholder analyses where the decision-making process involves coordinating views and intent, minimising the reliance on implicit assumptions can help identify inadequate uses of heuristic attributes, in both foresight and retrospect. It also maximises the utility of the adaptive toolbox (Gigerenzer and Brighton 2009), by tracing the historical perception and assumptions (memory), generates modularity in assumptions and better

transparency concerning inferences and uncertainty (feedback/reinforcement) and provides the ground for environmental calibration. Coupled with the previous sections, these factors can be used as a foundation of ontological and epistemological assumptions and constructs necessary for the formulation of a conceptual framework which reconciles the systemic and behavioural analytical perspectives. Once supplemented with an empirical/exploratory dimension, the conceptual framework can be used to guide the development of 'objective knowledge' constructs (i.e models) and heuristic strategies which adequately represent and address the cybersecurity management knowledge problem.

2.4 Emerging Concepts: Towards the Conceptual Framework

So far, both the organisational cybersecurity context-construct gap, and the knowledge problem it entails have been explored both descriptively, and as a function of fitness between prescriptive/heuristic constructs like risk management, the domain-specific complex ontology, and 'rationality' as a pragmatic heuristic for conceptualising contextual behavioural tendencies. These converging perspectives are used to describe and engage the research problem as a phenomenon and thus serve as an overarching conceptual framework. Conceptual frameworks are defined by Jabareen (2009:51) as "a plane of interlinked concepts" with each concept playing an ontological or an epistemological role. Furthermore, Berman (2013:3) presents their role and utility in their ability to: standardise the language used to address the research problem, determine the principles which underpin inferences, structurally support the organisation of content and conclusions, serve as theoretical/conceptual nodes, providing connection points with other theories, guide empirical research strategy and design, and aim to provide a coherent relationship between the conceptual and the empirical dimensions of study. In order to advance the empirical dimension of the project, the cross-granular nature of the core emerging concepts must be acknowledged and represented.

At a finer level of conceptual granularity, the postulated logic underpinning the organisational cybersecurity context-construct problem diagnosis entails the following framework:

Construct	Perspective/Dimension	Sub-constructs
Change	A dynamic view of the ontology of organisational cybersecurity management which reflects the emergent, cross-systemic, vertically integrated structures and interaction patterns. These are the drivers of systemic 'necessity', or 'adaptive tension', and underpin the dynamism and locality of the context faced;	• Complexity • Panarchy • Emergence • Adaptation

Rationality	A pragmatic view of the modus operandi of 'schema based' agents which considers cognitive and social adaptive mechanisms; This serves the dual role of conceptualising behavioural tendencies as part of an inference-oriented prescriptive 'schema' and considering the implications of (agent) decision-makers' tendencies as recipients of prescription. In this sense, 'rationality' is itself an object and subject of ontological dynamics;	• Representations • Inference • Heuristics • Biases • Norms • Roles • Culture
Knowledge	A contextually coherent, functional view of Knowledge as the precursor to inferential adaptation, which consists of conceptual and sub-conceptual (structural) representations of potential and actual systemic states, attributes, and tendencies;	• Critical realism • Pragmatism • Evolutionary Epistemology
Uncertainty	A complementary construction of Uncertainty as a state of hostility to adaptive inference which can emerge from epistemic and/or stochastic contextual attributes	• Likelihood • Heuristics • Contextual ecology
Risk	A risk-centric, contextual (organisational cybersecurity) exploration of the role of inferential/procedural constructs in conceptualising, modelling, and anticipating adaptive necessity;	• Vulnerabilities • Threats • Impact • Likelihood • Uncertainty
Adaptation	A converging, systemic view of adaptation as structural/behavioural change towards necessity — the central mechanism for navigating context dynamics while preserving emergent function/identity; Entails a decrease in adaptive tension.	• Aptation • Exaptation • Panarchy • Resilience • Change

Table 1. A Cross-granular 'Context-Construct' Conceptual Logic

Together, these interacting constructs provide a pluralistic, navigational logic for organisational cybersecurity efforts, while also presenting a complementary set of ontological

and epistemological assumptions. At a coarse representational level, they provide a structural blueprint of contextually relevant topics for empirical enquiry (elaborated in section 3.1). They also enable the examination and calibration of the otherwise abstract conceptual framing through its underpinning assumptions. Finally, once calibrated, the outputs of analysis can be used to employ the theoretical dimension of the study in a prescriptive output aimed to engage the effects of the research problem in organisational practice.

3. Methodology

The methodology section aims to use the outputs of the Literature Review as a platform for constructing an empirical research strategy to explore the notion of knowledge in a cybersecurity setting and its relationship to cyber risk practices. Using Contextual Constructs Theory, the first stage of the chapter entails formalising the project's point of view and using it to generate the research questions. This is followed by a discussion of research philosophy, which argues that Critical Realism provides a theoretically compatible, contextually adequate base of ontological and epistemological assumptions. The third sub-chapter covers the process of empirical research strategy development. More specifically, it explores methodological influences of the research philosophy, disciplinary tradition, research objectives, literature based conceptual framework, and pragmatic constraints. Subsequently, it identifies the single, exemplary, embedded case-study as a feasible methodological approach. The remainder of the research strategy formulation sub-chapter explores the case selection and design processes, as well as broader methodological considerations such as case/output validity. Finally, the fourth sub-chapter provides both a conceptual and a descriptive overview of the data collection and analysis processes, and of the specific outputs which underpin case building.

The previous chapters presented cybersecurity as a dynamic phenomenon which, when manifested within organisations, generates a local strategic problem. This problem is both epistemic, given the inferential mechanics of strategy, and systemic, as it emerges from the dynamics of system behaviour. A first methodological/investigative challenge presented by this narrative lies in the partial disciplinary agnosticism it yields. While Popper's (1978) three-world model of knowledge was used for structural coherence — i.e. guiding the analysis based on the locus of knowledge — the core problem 'diagnosis' emerges from the interaction of heterogeneous constructs. As a result, the study's methodology must account for the systemic, non-summative nature of the arguments put forward.

To address this issue, the chapter structure will be informed by Knight and Cross' (2012) 'Contextual Constructs Theory', which takes a systems perspective on the research process

and methodological design. This entails an exploration of the research context, the selection of constructs, and the interaction between the two. The context includes factors such as: the discipline of the study, the phenomenon/object driving the exploration, its theoretical background, the researcher, and the research problem, which embodies the researcher's approach towards the research object. Constructs within CCT are seen as building blocks required to assemble the research process. They serve the role of linguistically encoding concepts and phenomena which, within their defined context, carry the specific meaning that enables the development of the line of inquiry.

According to Knight and Cross (2012) such an exploration can be structured based on the four stages of the project's life-cycle:

1. The conceptual phase where the point of view of the project is determined based on the intersection between the researcher's perspective, the discipline of the study, and the methodological meta-disciplinary context of the phenomena under exploration;
2. The philosophical phase, where both the epistemology and ontology underpinning the project are established;
3. The implementation phase, which encompasses the research methodology;
4. The evaluation phase where the data generated is classified, analysed and used to extract the findings.

Each of the four stages builds on the previous in defining the research narrative. In spite of this, the four phases are not treated as inherently linear/sequential. Instead, they are seen as evolving and interacting based on the progression of the enquiry. Furthermore, for pragmatic reasons, not all aspects of the research philosophy are contained within, or introduced based on the linear chapter progression. For example, epistemological constructs are not just a passive dimension of the study, but also actively employed in both the problem diagnosis conducted in the early chapters, and in the prescription-oriented later chapters.

3.1 The Conceptual Phase

The problem at the centre of the study is twofold. In its pragmatic dimension, it identifies an inferential gap between knowledge availability and decision requirements in relation to organisational cybersecurity. From an epistemic perspective, this gap is critically explored through a risk-lens as a systemic function driven by non-linearity, behavioural heterogeneity, and inferential construct selection/adequacy. By emphasising a phenomenon-based view of cybersecurity, this diagnosis does not rely on, and is not conducive to a disciplinary interpretation of the problem area. Instead, it has evolved as various explanatory and prescriptive theoretical avenues failed to account for the indicators of significant epistemic limitations that managers face (outlined earlier in the study). Subsequently, a deconstruction of the 'knowledge-problem' was attempted based on Popper's locus of knowledge through a (complex, hierarchical) dynamic systems perspective. This, in turn, has introduced core notions such as scale, emergence, and adaptation in relation to the research problem.

However, as the systems-view provides little nuance in exploring the fine-grain, softer behavioural component of organisational behaviour, and the tendencies of actor driven top-down order, a cognition-oriented exploration of both individual and collective/social 'rationality' was introduced. A behavioural perspective is deemed meaningful within a complex system setting as social mechanisms and tendencies can shape interaction patterns which are either amplified or suppressed across the hierarchy. Furthermore, oversimplifications of agency are widely seen as problematic for models which aim to explain and assess the likelihood of given outcomes, i.e. risk. Thus, a nuanced interpretation of individual and collective behaviour as a foundation for assumptions is seen as paramount for understanding and bridging the diagnosed knowledge-decision gap. Finally, decision support systems and procedures are seen as a behaviour-guiding lens used to tackle uncertainty systematically. Most notably, risk constructs, in a plurality of manifestations, take a primary role as a procedural 'knowledge object' used to address the epistemic problem. A critical understanding of risk, in both the broader context of its application, and specifically within organisational cybersecurity is also deemed as an important component of addressing the driving problem of the study.

Thus, based on the research problem, three remaining (four in total) research objectives have been formulated:

0. Construct a literature based conceptual framework to represent the context-construct dynamics within organisational Cybersecurity;
1. Identify how Knowledge relating to Cybersecurity is produced, used and adapted at various levels within an organisation;
2. Critically analyse the role, and epistemic requirements of Cyber Risk Management;
3. Conceptualise a Risk based approach to address the Knowledge-Uncertainty dimension of cybersecurity management.

Together, these objectives enable engaging both the 'knowledge problem' and the 'context-construct gap' heuristics which guide the investigation. Objective '0' was achieved through the earlier stages of the study's construction and entails the development of the conceptual lens through which the problem is diagnosed. As such, it corresponds with the literature review, and is presupposed by the later objectives, which is why it serves as a foundational/implicit objective. Through the first objective, the context of cybersecurity 'knowledge' is explored. This entails a layer of theory driven analysis to functionally construct 'knowledge' within the emerging conceptual framework by exploring its attributes within the phenomenon of study. In addition, this objective also introduces the need for an empirical investigation to calibrate theory driven insights. Following an understanding of the function and form of knowledge in cybersecurity management/strategy, its relationship to Cyber Risk Management practice must be explored. Again, this entails a two-fold critical evaluation, i.e. theory and practice informed, and is driven by a recognition of (epistemic) context as a determinant for the adequacy of risk outputs. The final objective consists of employing the findings and insights obtained in a prescriptive, Risk-based framework which is theoretically coherent and accounts for the contextual tendencies of organisational cybersecurity. In the absence of a clear disciplinary context, these objectives ground the research point-of-view in a series of complementary constructs which were selected based on the problem diagnosis. For example, the study's pragmatic orientation is typical of organisational studies, in spite of the absence of such literature in the interpretation of the research-problem. This exclusion

was involuntary, based on positive-feedback in the identification of robust constructs which address aspects of the 'knowledge problem'. These constructs are also indicative of an implicit philosophical stance, and carry methodological implications, both of which will be discussed in the following sections.

A simplified relational logic of the problem's dynamics based on the conceptual framework building blocks elaborated in Section 2.4. is presented in fig. 2. This model aims to provide a high-level structural overview of the epistemic dynamics and serves a skeleton for further enquiry. In addition, it abstractly accounts for the interaction between constructs which belong to each of Popper's three worlds, thus providing a structural summary of the literature review.

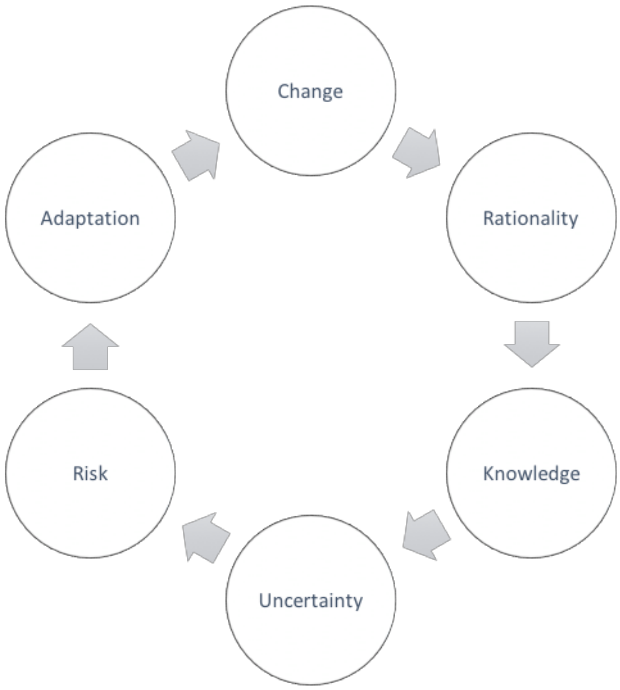


Fig. 2 Logic of enquiry: high-level overview

Given its role in guiding the empirical dimension of the study, the relational logic can also normalise construct granularity, which enables guided communication with heterogenous actors and data-gathering without enforcing a specific interpretation of each topic. 'Change' is a proxy term for complex system dynamics and provides a trigger for the knowledge problem. In a cybersecurity setting, change is continuous, and underpins the adequacy of defensive measures. 'Rationality' is a loose construct, contextually defined as the individual or collective worldview which corresponds to, and is affected by the Change. 'Knowledge' is

a function of Rationality and enables adaptive-action formulation. However, it is also an inherently incomplete, limited, and context-bound construct. 'Uncertainty' is seen as a contextual limitation of knowledge which results from the complexity and pace of system dynamics, and from insufficient knowledge. 'Risk' is an objective knowledge lens through which a 'known-unknown' segment of the change is accounted for within the world-view. Finally, 'Adaptation' accounts for both intentional adaptive measures taken under residual uncertainty, and hard adaptations which are environmentally imposed and represent a release of adaptive tension. As this final construct also entails a form of meaningful change, it serves as a driver for the following cycle. Despite its relative lack of nuance, this simple model illustrates the key aspects of the knowledge problem narrative, and helps structure the empirical enquiry highlighted in the research objectives.

3.2 Research Philosophy: Contextualising Critical Realism

Given the framing of the research, i.e. cybersecurity management as a knowledge problem, some core philosophical stances have permeated the narrative at an introductory stage. Nonetheless, the following section will make both the ontological and the epistemological grounding explicit to elaborate and justify the study's philosophical positioning and its implications. This exploration of the research philosophy also heavily influences the selection of research methods used to conduct the empirical dimension of the study. It is worth noting that the current section is primarily centred on the ontology-epistemology dynamic, as opposed to secondary dimensions of rhetoric which do not directly support the achievement of the research objectives.

3.2.1 Ontology

So far, the ontological underpinnings have been implicitly introduced through constructs such as complex systems, adaptation, emergence, interactions, agents, and knowledge objects. These notions are indicative of critical realism (Wynn Jr. and Williams 2012, Zachariadis *et al.* 2013), despite differences in their ontological status (i.e. physical vs. informational). A critical realist ontology is underpinned by three core assumptions: the existence of an observer independent reality; the existence of necessity, whereby objects present both distinct powers/tendencies and susceptibilities; and, the stratified and differentiated nature of the world, which contains objects and structures with the ability to create events (Easton 2010). Each of the three assumptions will be critically explored in relation to the emerging narrative, to support this philosophical stance.

The existence of an observer-independent reality is consistently assumed across the spectrum of ontological realism and is inherent in applications of complexity theory. In fact, Merali and Allen (2011) present the existence of explicitly identifiable (i.e. distinguishable) systemic entities as an axiomatic underpinning of system thinking, alongside their structural composition of interconnected parts which collectively yield non-summative properties. This presumes observer-independent, and even context-independent structural/ontological

regularities linked to generative mechanisms. Within Critical Realism, mechanisms are seen as "the way of acting or working of a structured thing […]" which has "causal or emergent powers which, when triggered or released […] determine the actual phenomena of the world" (Lawson 1997:21 in Zachariadis *et al.* 2013:3). Thus, within the conceptual framework, this first pillar of (critical) realism is implied through the use of postulated ontological mechanisms like evolutionary selection and systemic adaptivity as drivers of the research problem. Despite the epistemological implications of their social construction as concepts, the mechanisms underpinning these abstractions are addressed as observer-independent, and described by Tsang (2014) as intransitive objects of knowledge. While the argument for an ontological plurality/stratification is also recognised (Klein 2004, Popper 1978), non-exhaustive intransitive elements are seen as manifested generally. In this sense, physical and social reality present epistemological differences, yet are fundamentally converging domains of enquiry when exploring a phenomenon-based view of organisational cybersecurity. This space of convergence is the ontological core of adopted constructs such as the Panarchy.

The second and third ontological assumptions pertain to 'objects', or 'entities' with heterogenous yet distinguishable attributes, which tend to form structures through internal relationships and practices (Easton 2010). Furthermore, these relationships are the basis for the identity of entities (Tsang 2014). Unlike variables which are measurements, entities are the object of measurement, and serve as explanatory building blocks (Easton 2010). Observable behavioural expressions of mechanisms through entities and structures form events (Wynn Jr. and Williams 2012). Dynamic systemic structures are underpinned by interacting entities across scales of emergence, i.e. if described in a single dimension, markets are structures of commercial entities, organisations are structures of actors. Adaptation is, thus, a function of entities that are undergoing changes which prevent the collapse of their relational identity. In this context, both the occurrence of adaptive change and systemic collapse are events. Furthermore, the nested/stratified nature of structures, expressed in the conceptual framework in the form of systemic hierarchies, entails existential interdependencies across structures.

Bhaskar (2008) identifies three domains within critical realism: The Domain of the Real, of the Actual, and of the Empirical. The Domain of the Empirical encompasses events which have

been observed, making it uniquely experiential. The domain of Actual is an expansion of the Empirical and includes the totality of events. Finally, the Domain of the Real contains the mechanisms which yield the patterns that form events. This distinction is unique to critical realism and shapes its interpretation of causality. More specifically, based on this distinction, observation is deemed insufficient for the extrapolation of causal laws, which are a product of the Domain of the Real. A more pragmatic use of causality is presented by Easton (2010:120) in the form of "causal powers and liabilities". The former describes the ability of entities to cause events while the latter describes a "susceptibility to the action of other entities". So, within the current projects, cybersecurity vulnerabilities are a form of causal liability for organisations, and a causal power for threat actors.

The limitations of the empirical (domain of) observation as a basis for extrapolating ontological regularities as causal laws are amplified within complexity theory. On this point Juarrero (2011:161) notes:

"Although causes and effects cannot be the same in all respects, traditional views of causality also assumed that similar causes, under similar conditions, always produce similar results. The nonlinearity of positive feedback and circular causality present in complex systems vitiates these two assumptions. As a result, a different logic of explanation becomes necessary. When nonlinear interactions cause interlevel relationships like those described above, the meaning of individual events can be understood only in context: in terms of the higher-level constraints (the dynamics) that govern them. Those higher-level constraints, in turn, are produced by the very interactions occurring at the lower, particulate level. The logic of explanation of hermeneutic narrative and storytelling is therefore more appropriate for phenomena whose very nature is a product of the strange causal circle between whole and part, with feedback tentacles reaching out into the environment and back in time."

Thus, given the conceptual framework used to tackle the research problem, the importance of recognising context is paramount. In this sense, the correlation of patterns under complexity, at the expense of context, is inconsistent with the ontological arguments put forward. It is also worth noting that the effects of randomness, i.e. chaotic system behaviour,

driven by interactions amongst entities, are prone to causal disproportionality, particularly when accounting for the non-linearity and limited scale-constraints which characterise the cyber domain. This point illustrates that randomness and order are simultaneously actual (Tsang 2014) and experiential phenomena — the gap between the two lying between Bhaskar's (2008) domains. The former involves degrees of informational entropy, while the latter is a product of, or nested within agency.

Subsequently, the inherent duality of patterns and regularities as measures of order emphasises the epistemological significance of social objects as ontological entities surviving based on a 'schema' of both their internal and external reality (Maguire 2011). Given their inherently simplified nature ('the map is not the terrain'), models of reality present a significant scope for the perceptual distortion of patterns. Furthermore, this duality also grounds the meta of the current discussion, as the desired output of the research is itself a social product, nested within function-specific, 'necessity' oriented structures (i.e. organisations). It is this necessity, as highlighted by Easton (2010), that sustains the cohesion of these structures. The pragmatic implications of this idea are further described in the following section, particularly for 'knowledge' as a construct.

3.2.2 Epistemology

As a post-positivist philosophy of science, the Critical Realist epistemology is derived from its ontology and its response to the critique of naïve positivism. This emphasis on ontology is used by Klein (2004:130) to (critically) characterise it as a "primarily ontological" stance with "epistemological implications". Nonetheless, these epistemological implications are significant as they enable accounting for the role of social construction without abandoning the tenets of realism. Furthermore, given the dual ontology of organisational systems which is central to cybersecurity as a phenomenon, focusing on the social domain at the expense of the physical would yield an incomplete perspective. Indeed, agency, knowledge objects, and 'soft' social variables are meaningful aspects of the problem. However, these are complemented by an overview of systemic mechanics, network effects, ontological hierarchy, emergence and adaptation — all of which describe mechanisms of the Real. While their

description is socially constructed, and seen as fallible, their observer-independent underpinning of regular ontological mechanisms is not. Furthermore, Easton (2010) highlights that the interpretation of social phenomena depends on concepts, and goes beyond a material explanation, towards establishing meaning.

An overview of the Critical Realist conception of Knowledge is provided by Bhaskar (2008:15) who identifies it as 'Transcendental Realist'. As a construct, knowledge is thus only passively defined based on its objects (i.e. "structures and mechanisms"), and its process ("social activity of science"). Bhaskar (2008:15) notes:

"… (Transcendental Realism) […] regards the objects of knowledge as the structures and mechanisms that generate phenomena; and the knowledge as produced in the social activity of science. These objects are neither phenomena (empiricism) nor human constructs imposed upon the phenomena (idealism), but real structures which endure and operate independently of our knowledge, our experience and the conditions which allow us access to them. Against empiricism, the objects of knowledge are structures, not events; against idealism, they are intransitive…"

While the absence of definitions of knowledge which are both explicit and differentiated is a source of criticism (Klein 2004), the Critical Realist conception of knowledge emerges as a function of its ontological claims. Given its dependence on social processes and agency, knowledge is both prone to errors, and theory laden (Easton 2010) — an unavoidable side-effect of bound perception (Mark et al. 2010). Furthermore, it is functionally linked to the 'schema' of reality upon which the survival of social entities is predicated (Maguire 2011). The hierarchical, coevolutionary nature of social ontology, and its reliance on foresight and intent, communication, and technology (Holling 2001) shape the evolutionary incentive for epistemic specialisation (Laland *et al.* 2000), resulting in both an individual, and a relational locus of knowledge. In other words, while beliefs, justifications and epistemic outputs can be, and generally are properties of individual agents, their meaning, utility, and role in action are generally functions of their wider epistemic/systemic context.

Based on these premises, two partly divergent yet reconcilable points can be raised: statements, beliefs and externalisations of epistemic schemas can be interpreted as ranging

from true to false based on their correspondence to observable aspects of reality (realist stance); and, from a navigational perspective, the utility of knowledge for social entities and structures is not linear, summative, nor is it inherently a product of its truth-value, though the two may be linked (pragmatism). Given the social context of the current enquiry, the overarching epistemological stance is indeed a critical realist one, which acknowledges 'truth seeking' as a non-absolute, limited, yet meaningful arch-objective. This includes the exploration of Real mechanisms within the context of the research problem. However, the prescriptive component treats knowledge as nested within an organisational setting, which operates as a function-oriented system with clearly delineated necessities. Thus, in this dimension of the project, the pragmatic utility of knowledge construction will be emphasised in response to the priorities of its (organisational) social context.

Another epistemological aspect which results from the premises of Critical Realism consists of the positioning of knowledge boundaries — the unknown. Employing a complex system framing when examining a phenomenon is an epistemological choice which conflicts with its reducibility, predictability, and platonic essentialism (Gershenson 2013). Furthermore, the path dependent, evolutionary nature of knowledge building processes is also recognised. This is particularly relevant for the pragmatic exploration of cross-domain, complex, dynamic phenomena which are not solely the product of regular mechanisms, but also of cross-scale interactions manifested locally. So, a critical understanding of the inherent constraints to knowledge must precede and guide the process of empirically grounding prescription. This objective is addressed by exploring the dynamics of structure/system necessity and intent, as well as the relationship between Real mechanisms and inherently bound navigational schemas.

3.3 The Implementation Phase: Building the Methodology

3.3.1 The Methodological Implications of Critical Realism

Without a clear disciplinary context, the research design and method selection are driven by the problem framing, the research objectives (questions) and of the philosophical position. As these aspects have been elaborated in the previous sections, the role of empirical enquiry can be demarcated and used to infer a methodological toolkit.

Firstly, the Critical Realist stance provides an overarching logic of empirical enquiry — the meta. From this position, the ontological regularities required for theoretical generalisation are explored as a product of mechanisms, which are distinct from the empirically accessible events they yield. As a result, abductive/retroductive logic is used in Critical Realism to investigate reality across layers from the perspective of its underpinning mechanisms and structures (Tsang 2014). Subsequently, retroduction entails a departure from the sole focus on the domain of the Empirical, in the process of developing meaningful explanations (Reichertz 2014). Based on this commitment, Critical Realism is described by Tsang (2014) as a largely a method-agnostic philosophy which places emphasis on the inherent complexity of the Actual, and the existence of the Real. From a critical realist stance, developing knowledge about organisational cybersecurity requires a retroductive, stratified account of the mechanisms driving the accounts of the Empirical. This, in turn, favourably positions methods able represent and account for nuance, a layered target segment of reality, and complexity in the convergence of the physical and the social domains. Finally, the Critical Realist commitment to objects rather than variables entails a reluctance to abstract measures as the focus of the investigation.

"… the critical realist view on causality should not be about a relationship among distinct events (e.g., the fact that event "A" by and large has been followed by event "B") but about realizing the process and conditions under which "A" causes "B," if at all." (Zachariadis *et al.* 2013:3)

Secondly, the parameters (assumptions) of the research problem also constrain the range

of adequate methods of enquiry. The research problem treats organisational cybersecurity as a complex, applied phenomenon which is anchored in its setting of manifestation. This anchoring leads to an interpretation of 'actual' cybersecurity events as heterogenous and causally local, while also manifesting (general) mechanisms. Thus, events in this setting, unlike their underpinning mechanisms, are treated as limited in epistemic generality. An example of this distinction lies in the potential locality of the chain of behaviour triggering a specific breach, as opposed to the wider general mechanisms which yielded the event, i.e. poor risk management, myopic organisational priorities, ineffective representational models, exploitation of asymmetric knowledge. Furthermore, organisational adaptive pathways are explored through the relationships between cybersecurity knowledge, uncertainty and risk constructs, cross-scale interactions and functional hierarchies (structure), as well as systemic and social dynamics. Such an exploration requires an adequate, homogenous, and well-defined research context which can be investigated across functional dimensions: panarchy/grander context (includes stakeholders, competitors, and threat actors); the organisation (system of focus); the function of cybersecurity (which can be structurally divided).

As a result, the purpose of the empirical dimension of the study is the exploration of the topics supporting the previously introduced simplified relational logic of the problem's dynamics (fig. 2.) from a variety of stances. These stances are established as relative to cybersecurity risk management as a function. Capturing nuance under complexity, while critically investigating the empirical adequacy of the conceptual framing and of the study's core assumptions are both central to data collection. This entails a qualitative investigation of complementary narratives across layers in a homogenous setting. Based on the totality of requirements, stances, and considerations brought forward, the case study emerges as a philosophically and pragmatically appropriate method of empirical enquiry.

3.3.2 The Case Study in Cybersecurity Management

An immediate consideration when constructing an empirical strategy centred on the case study consists of ensuring its suitability within the overall research design. The compatibility

between case study research and Critical Realism is highlighted by a range of authors, including Easton (2010), Wynn Jr. and Williams (2012), and Tsang (2014:177), based on a shared open systems perspective, and due to the view that 'closure conditions' are a rare outcome in social scientific enquiry. These two points are also used to illustrate the inherent predictive limitations of theory in social science, given the absence of closed, controlled systems. Indeed, the main utility of the case study as a method lies in its explanatory power under contingent, irreducible conditions. It enables maintaining the holistic attributes of complex (social) phenomena, as manifested in their context of study, making it a versatile, yet not all-encompassing methodological tool (Yin 2003). However, case study research is not uncontroversial. Broadly, concerns over the method either address procedural tendencies which can negatively shape the output of such research, or, more fundamentally, question the validity of case-studies for knowledge building (Flyvbjerg 2006, Diefenbach 2009).

Amongst the central points of critique addressed to case studies as a method of social enquiry lies the issue of generalisation, which is conceptualised as a function of population representativeness (Tsang 2014). Reichertz (2014) describes generalisation as the process of projection for the characteristics of a selection of elements (sample) as representative for all the elements of the group (population). Given that case studies present a trade-off between the depth and the breadth of study, proponents of the assumption that the number of observed elements is the basis for both the generality and the non-local validity of findings are likely to find the method lacking. This is largely a function of philosophical stance. Tsang (2014:183) highlights this by differentiating between a Positivist, Intepretivist, and a Critical Realist approach to empirical, as well as theoretical generalisation. Under Critical Realism, cases are presented as useful for both identifying "demi-regularities" which serve as a precursor to theoretical development, and for acquiring information concerning the contingent behaviour yielded by ontological mechanisms. Furthermore, case studies provide the opportunity to validate and adjust theories by comparing and adapting postulated mechanisms to those indicated by the case data.

Nonetheless, it is important to acknowledge the potential for divergence between methods rooted in a quantitative logic of representativeness, and case selection procedures. Due to the emphasis on qualitative depth, context, and locality, case-study research is more likely to

focus on specific instances and their attributes, at the expense of capturing a substantial, quantitatively significant sample from a given population. The importance of this potential trade-off depends on the research context and objectives. More specifically, when attempting to identify the attributes of a population, case study research may prove to be a useful, yet insufficient/incomplete tool for generalisable findings – i.e. based on a representative sample. In contrast, when attempting to gain a substantive understanding of complex, locally anchored phenomena or events, the absence of volume-based sampling procedures is less likely to have a detrimental effect on theory building. As a result, the methodological adequacy of case studies is largely shaped by the disciplinary, philosophical, and operational framing of the research context. Finally, Flyvbjerg (2006) highlights the importance of the "strategic choice of case" as a determinant of the generalisability of subsequent findings. This is predicated on the claim that observations from exemplar or revelatory cases can be used to infer behaviours and tendencies from intermediate cases (Flyvbjerg 2006, Diefenbach 2009)

The second dimension of criticism towards case studies relates to specific procedural tendencies which can affect the validity of the findings. Unlike the previously highlighted concerns over generalisation, procedural tendencies are not inherent, and can be largely mitigated against or avoided altogether. Diefenbach (2009) identifies a series of such concerns which cover the absence of an 'objective', fixed, scientific research design process; the potential for a non-systematic data selection and collection process that can be biased by the researcher; and, internal validity issues due to problematic, insufficient data which is not analysed through 'objective' means. It should be noted that these points of criticism are also grounded in a specific philosophical and procedural framing, favouring a (post)positivist approach to social sciences. While Diefenbach (2009) addresses each of the highlighted concerns at an abstract level, within the context of the current research narrative, these tendencies are addressed systematically throughout sections 3.3.3 and 3.4.

Beyond philosophical considerations, method selection in research strategy development is a function of three factors, according to Yin (2003). These are: the nature of the research questions, the degree of investigator control over behavioural events, and the focus of the enquiry on either contemporary or historical events. Case studies are presented as

appropriate in instances where the research questions fall under “how” and “why” explanatory archetypes, while the investigation is not predicated on behavioural control, and its focus lies in contemporary events. By applying this conceptual lens to the current enquiry, the empirical research objectives address the “how”: how cybersecurity knowledge is produced, used and adapted across organisational layers; and how cyber risk management is conditioned epistemically in an applied setting. Additionally, the setting of interest is inherently contemporary, given its role in establishing prescription, while the empirical enquiry, manifested through data collection procedures, does not aim nor is it able to shape the behaviour of the research objects. Instead, a largely passive, observational perspective is needed to achieve the explanatory outcomes of the study.

Exploring cybersecurity as a phenomenon entails construct flexibility, as it is manifested across functional layers within an organisation. For example, the experience of operational actors who rely on cyber infrastructure with the topics of enquiry is meaningful, yet potentially different from that of information security specialists, or organisational policy makers. However, exploring any such population in abstraction of its context inherently limits the explanatory potential of the enquiry. Thus, a holistic perspective of cyber risk, knowledge, and adaptation must account for the internal dynamics, tendencies and perceptual disparity throughout the layers of cybersecurity management as a function. Furthermore, given their emphasis on observational depth rather than breadth, case studies enable outlining the context of the enquiry — a key component in accounting for contingency. This includes considering measures of financial performance, macro-context, industry/sector specific variation and tendencies, role of cybersecurity in the operational model, staff base, capabilities, strategic direction, and so on. It should also be noted that some core constructs of the investigation, like the link between knowledge and the application of risk constructs, are not transmutable. As both entail local accounts and implementations of otherwise abstract constructs, there is significant scope for context specific contingency as a driver of event variation. Internal analytical consistency is therefore paramount.

In addition, there are also pragmatic considerations which support the effectiveness of the case study as the main empirical method of the project. Firstly, given the sensitivity of organisational cybersecurity as a topic, the selection of a broadly defined, cross-

organisational range of participants carries efficiency and analytical costs. The former is attributable to constrains on participant selection strategies, like snowballing (Saunders *et al.* 2014), and gatekeeper plurality. The latter results from the inherent lack of horizontal population homogeneity assumed by the conceptual framing, and by the relative absence of structural and functional standardisation for cybersecurity management. Furthermore, without a plurality of perspectives which share partial environmental consistency on the topics of enquiry, the truthfulness, completeness, and depth of varying perspectives cannot be accounted for. Also, given the substantial volume of survey/aggregate data on organisational cybersecurity, and the relative deficit of in-depth, phenomenon oriented qualitative studies, there is a scholarly opportunity for substantive, case contributions.

Such contributions are also compatible with the main research traditions which are used to construct the research narrative. In contrast, within the current context, techniques such as Agent Based Modelling that are employed in complexity studies were found to be reductive and unable to represent social and behavioural context and nuance. Experiments, focus groups and questionnaires have also been considered, however they were found to entail a disconnect from the systemic context, and to offer limited insight into 'real world' cross-hierarchy interactions and phenomena. Additionally, the notion of a rigid conceptual structure prior that precedes data collection is met with reluctance, given the relatively broad findings of the literature review. In contrast, ethnographic research presents contrasting limitations: the absence of a theoretical foundation, which can impede on the explanatory and prescriptive potential of the study; and the limited presence/absence of previous ethnographic studies encountered in the main disciplinary traditions covered throughout the literature review. So, out of a broad range of methods which have been considered, (and attempted) throughout the duration of the research process, the case study emerged as a versatile and contextually compatible alternative, in spite of its potential and actual limitations. Attempts to mitigate against such limitations are described at length throughout the following sections, and inform case selection, the primary and secondary data collection and analysis processes, and the case narrative construction.

The current section can be loosely summarised through three points: despite its limitations, the case study as a method is found to be adequate for the current enquiry, given its

philosophical and methodological grounding; subsequently, it has the ability to yield the empirical narrative coherence that is necessary for postulating (and prescriptively employing) ontological mechanisms through retroduction; and, the exploration of context verticality, which is manifested through systemic/functional layers, is an important driver of this ability. In the following section, the issues of validity and insight potential for the research narrative will be discussed as functions of case selection and design.

3.3.3 Hierarchy and Verticality: Case design

3.3.3.1 Questions and Propositions

Despite their implementation heterogeneity, case studies share an overarching pattern in their design (Yin 2003). This includes an explicit set of Questions and Propositions, a defined Unit of Analysis, the logic link between Data and the Propositions, and the basis for interpreting the study's findings. The questions guiding the process of data acquisition reflect the first two objectives. These are:

- How is Cybersecurity Knowledge produced, used, and adapted at various (functional) levels within an organisational setting?
- How is Cyber Risk Management used, and conditioned by available knowledge/epistemic constraints?

These questions entail empirical nuance, and are responsive to narrative as a means to anchor the conceptual/theoretical framing. They are also supplemented by several underpinning propositions which guide the enquiry process.

Within the questions, a dynamic, relational and hierarchical view of organisational knowledge is embedded. 'Cybersecurity Knowledge' is introduced as a contextually distinct epistemic construct, with meaningful manifested variations based on its locality. This means that epistemic efficiency and performance in cybersecurity, as a subsection of overall organisational performance, entails adaptations in form and content which serve its various specialised contexts of application. A knowledge-based view of cybersecurity management

also provides the basis for an epistemic functional division of cybersecurity actors. Thus, rather than taking a central, or departmental perspective of organisational cybersecurity, such a division explores the actor structures which shape systemic performance. This entails distinguishing between the *Operational Actors* which engage with the cyber infrastructure for value creation yet are not in security specific roles; *Risk Analysts*, who employ risk constructs to supervise, communicate, and address risk tendencies; and *Decision Makers*, who can shape policy, impose infrastructure changes and instil top-down change. All three categories of actors shape an organisation's cybersecurity, however they do so in meaningfully different ways, with different epistemic requirements.

While not based on a specific, pre-existing taxonomical division of organisational cybersecurity knowledge functions, the three interacting categories are expected to show meaningful differences in their respective epistemic contexts. More specifically, the group-based division aims to acknowledge the relationship between: the operational dimension of risk, and respectively knowledge, through their effects on both actors and processes; the procedural dimension, where formal risk analysis is conducted and integrated in function specific representational models; and, finally, the strategic/policy dimension which guides top-down efforts, and must address cyber risk in the wider organisational performance context. In isolation, data derived from each individual group can yield a myopic perspective of in-case dynamics. However, collectively, they enable a holistic exploration which includes both top-down and bottom-up phenomena and interactions through hierarchical layers, in accordance with the theoretical framing of the research problem.

Potential limitations which can emerge from such a categorisation are acknowledged, and include: added constraints on the participant pool due to a necessity to shortlist for organisations with an explicit cyber risk analysis function; a detrimental effect on the feasibility of comparative studies due to inter-organisational functional differences across these three dimensions; and a potential imbalance between the three respective populations given their inherent asymmetry. Nonetheless, as an initial proposition, the participant grouping provides a meaningful epistemic distinction between interconnected yet distinct actor clusters which interact to shape the core facets of cybersecurity as an organisational function. This enables further focusing the data collection process in a manner that is

consistent with the theoretical framing of the study. As a result, the highlighted constraints are implicitly considered throughout the following sections, most notably in the processes of case (3.3.3.2) and participant selection (3.4).

A second set of propositions was introduced through the relational logic of the core constructs (fig. 2), which illustrate the research problem based on loosely defined ontological and epistemological mechanisms. These narrow down the range of potential topics of enquiry and introduce a literature-informed cyclical logic of demi-regularity for organisational cybersecurity management as an adaptive, epistemically driven practice. They also expand on the link between knowledge, risk and adaptation by incorporating systemic change which serves as the object of epistemic adaptation, 'rationality' as the arch-structure of agency, and residual (or inherent/stochastic) uncertainty as the object of risk constructs. Together, they support the investigation of a dynamic, evolving view of knowledge which is explored through the first research question, and is assumed within the second. These propositions guide the case design by localising and structuring both the necessary data and the analytical approach that is required to address the research questions. More specifically, they position the objective of the emerging empirical enquiry as the engagement of agents across the functional division of cybersecurity risk in a homogenous (and exemplary) setting, on the topics introduced through the relational logic of the problem. This must also be coupled with context data which is needed to delineate contingency and locality, in an attempt to distinguish potential explanatory mechanisms.

3.3.3.2 Unit of Analysis and Case Selection: The Single, Embedded Case Study

Another aspect of case design which follows this line of methodological framing consists of defining the Unit of Analysis — or, simply put, what the case consists of. Furthermore, as the case questions are addressed under a relatively loose organisational framing, the choice of a single or multiple-case strategy must be made, and the actual setting of the case must also be determined. Based on the propositions and the case questions, the case itself is an organisation’s cybersecurity and risk function, in an internally stratified manner. This stratification leads to what Yin (2003) describes as embedded units of analysis (each proposed

cluster of participants) which converge to form the case, supplemented by context inputs. As a result, given the reliance on retroduction, the stated role of empiricism within the philosophical stance, the absence of preceding exploratory work which could guide the comparative logic of multiple case studies, and the importance of hierarchical consistency and systemic homogeneity, a single, embedded case study is preferred. In addition, ontological regularity, and access symmetry — both drivers of effective comparative studies, are seen as not applicable within the context of the study. In fact, the emphasis on analytical depth, the assumed empirical event causal-chain specificity, and the epistemological assumptions yield a prevalence of single case study/limited number of cases under the Critical Realist paradigm. On this point, Wynn Jr. and Williams *(*2012:804) note:

"The distinguishing aspect of intensive case selection in CR is the focus on exposing the causal processes, expressed as causal mechanisms, which have produced a unique set of events and the specific structural/contextual factors that combined to generate them. As such, the results are not typically or necessarily generalizable across multiple contexts so that case selection is not made on this basis. The emphasis is on the detailed and precisely focused study of a limited number of cases, often a single case, in a specific setting in an attempt to build an explanatory theory that matches the empirical facts as closely as possible. […] This intensive study of a particular setting often results in an in-depth, contextually relevant analysis of a complex organizational process…"

In light of this, a single, vertically embedded case is deemed as methodologically appropriate given the research design. However, a key issue of single case studies is the case selection process. The "strategic choice" of a case is highlighted by Flyvbjerg (2006:226) as a source of external validity in a social sciences context. An ability to postulate ontological mechanisms from events and observations presents challenges, especially for the identification of strictly local phenomena and dynamics, and for the explanation of systemic performance with consideration for contingency. As a result, the process of case selection must only shortlist institutions whose cybersecurity dynamics are not likely to be driven by local limitations, considerations and factors. A desirable case setting must exhibit a substantial informational asset base, and a reliance on cyber infrastructure for its operations. This condition selects against organisations which do not perceive cybersecurity to be an operational imperative, or

can justify disregarding cybersecurity concerns under pragmatic grounds. Such organisations are likely to have an inherent epistemic handicap relating to cybersecurity while events and occurrences in such a setting are unlikely to be illustrative of domain specific mechanisms and dynamics. The second condition relates to the existence of capital surplus, or evidence of financial health. Capital constraints are also a likely cause for pragmatically under-prioritising cybersecurity. Organisations with both financial flexibility and a significant informational and infrastructural asset base not only have the justification for pursuing cybersecurity as a matter of sustainability, but also have the means to conduct investments and changes that are deemed desirable. Thus, their domain-specific performance is not capped by financial limitations. A third condition consists of the existence of an active threat climate. Selecting against organisations which do not perceive the pressure of threat actors ensures that, within the case, not only there is a valuable asset-base and cyber infrastructure to defend, as well as the means to do so, but also that there is someone to defend against. Finally, in line with the previous conditions, a desirable case setting must exhibit a distinct capability, or know-how, in cybersecurity practices. The resulting organisational profile creates a best-case scenario whereby events and approaches are not the product of absent vulnerabilities, threats, capabilities or resources. Such a setting is likely to be exemplary of domain dynamics, yielding an opportunity to examine and engage the topics of enquiry.

In addition to these theoretical selectors, a pragmatic ability to gain adequate access and pursue data collection is an inherent condition of case selection. Other secondary yet desirable attributes include the availability of sufficient context data, comparative performance visibility, and measures of sector specific contingency. Together, these factors describe a 'critical case' under Yin's (2003) classification. Such a setting presents an opportunity to study epistemic dynamics which are not hindered by, or a product of local operational or perceptual limitations. Furthermore, it enables a critical analysis of the life-cycle of risk constructs based on the perspectives of practitioners with demonstrable motivation, means, and know-how in cybersecurity management and strategy.

Based on these factors, University X has been selected as an appropriate case setting. Its operational model is informational-asset dependent, while heavily relying on its cyber infrastructure. Furthermore, it is highly susceptible to reputational damage in the event of

cybersecurity incidents. The non-monetary value of data assets is also worth highlighting as the institution's data stream can include both secret and sensitive data from a wide variety of partners/stakeholders. Financially, the institution is a high performer (first quartile) in sector-specific comparative terms. Indeed, the institution also faces an active threat climate, a point which was confirmed in preliminary discussions. Such a threat presence at a sector level is also to be expected, based on existing secondary sources. Romanosky (2016) identifies Educational Services as having the second highest incident rate by industry, following Government, and fourth highest number of incidents in the considered data, after Finance and Insurance, Health Care, and Government. While the data-set is not specific to the UK, this serves as an indicator of sector-wide threat presence. As the last conceptual qualifier, University X is linked to know-how in cybersecurity from both an academic and an applied, commercial spin-off venture perspective. Additional comparative attributes and qualifiers as well as the context data for University X are described at greater length in section 4.1.

3.3.3.3 Defining 'Data'

From a data perspective, case studies are not restrictive, as they can accommodate a range of alternative data collection and analysis methods which provide an account of the units of analysis based on the study's questions and propositions (Yin 2003). However, in spite of this flexibility, preferences and tendencies can be observed. For example, one of the most common approaches in case study data collection is the semi-structured interview (Easton 2010). Indeed, Brinkmann (2013:21) describes semi-structured interviews as "probably […] the most widespread ones in the human and social sciences…". They are presented as enabling greater levels of focus and, ultimately, greater control over the interview process than unstructured interviews. However, they also provide more leeway for narrative adaptation and conversational follow-ups than structured interviews. This versatility is advantageous for the current line of enquiry.

As the collection of organisational data concerning the main topics of interest presumes the participation of diverse actors, interviews are one of the main available tools for the task. Additionally, while the line of enquiry does require a focus on core constructs, it also aims to explore variation in interpretation and experience. The semi-structured interview format

enables a responsive approach which can account for nuance, contradictions, clarifications, and adaptation. It also allows for a narrative convergence using experientially distinct populations. This is valuable given that, while participant clustering is primarily based on the functional division of cybersecurity previously introduced as a proposition, cluster homogeneity is not assumed. Thus, the topics of enquiry can be adapted based on the interviewee's role, experience and worldview — all of which important when attempting to generate meaning from the data. Through such adaptations, the interview questions can accommodate participant contingency while also being linked to the logic of enquiry and the conceptual framework.

It should be highlighted that the common reliance on interview data for case building has been the subject of criticism questioning the suitability of the method (some of which covered in section 3.3.2.). Most notably, Diefenbach (2009) highlights a series of such concerns within the literature, addressing various aspects of interview outputs. These include the internal validity of interview data, and its argued (in)ability to reflect objective reality; the low volume of observations generally associated with interviews; and, their 'snapshot' character' in circumstances where longitudinal development is central to the research problem.

Within the current project, the adequacy of semi-structured interviews has been considered in two dimensions: absolute – i.e. context independent validity of the method, and comparative – context dependent validity, in relation to alternative available methods. From an absolute perspective, the semi-structured interview is compatible with the critical realist grounding of the study, which does not equate the 'empirical' ontological domain with the 'real'. As a result, from this perspective, an inability to fully reflect objective reality, i.e. the real, is assumed across the range of empirical data collection methods, albeit with variations based on the research context. Subsequently, the interview data is not seen as inherently invalid or flawed. From a comparative merit perspective, based on the emerging research strategy, the number of observations is largely constrained by a mix of case attributes, i.e. number of relevant participants within the organisational structure, and operational constraints, i.e. data-collection cycle deadlines, informant availability and willingness to participate, and the overall organisational context – operational climate, cycles, and key events. As a result, interview data was not perceived as a comparatively limiting format in

terms of the number of observations, and the time sensitivity of the phenomena under observation. To further mitigate against these factors, a series of steps were taken, including: the use of additional sources of secondary data which can provide a historical context; the attempt to recruit heterogenous participants based on role and background; and the acknowledgement of time spent in the organisation as potentially significant. Based on the above, semi-structured interviews were found to be an appropriate primary data collection format for the emerging case study.

Unlike the internal case data, the development of an in-depth account of the case context presents a greater opportunity for data diversity. In accordance with the philosophical and conceptual emphasis on 'layers' of reality, the case context must illustrate the nature and implications of sector-specific contingencies, and how both the case and the wider sector fit, from a cybersecurity perspective in a national setting. In order to achieve this objective, a variety of data sources are used in Section 4.1, ranging from descriptive open data sets, reports, surveys, and anecdotal accounts from the institution, sector-level bodies, as well as governmental and private enterprises. Again, the resulting description aims to converge with the primary data and support its interpretation/meaning generation process. An in-depth, retrospective account of the data collection, processing and analysis stages is provided in the following chapter.

3.3.3.4 Interpretation of Findings: Linking Data to Propositions

The final stages of Yin's (2003) arch-structure of case design address the issue of the interpretation of findings, and the linking of the data to propositions. Given the form fluidity of 'data' in case studies, little method-specific guidance can be provided, other than anecdotal evidence of successful approaches. However, the lack of accepted methodological orthodoxy is not inherent to case studies. Maxwell and Chimel (2014) highlight this point within the context of qualitative methods in general, as the links between data are more substantive rather than formal in nature. Substantive relations focus on interactions, whereas formal relations focus on similarities and differences. In response to this distinction, qualitative data analysis in case studies, particularly embedded, exploratory ones, can be associated with what Maxwell and Chimel (2014) describe as 'connecting strategies'. These include matrices,

which have a tabular structure, and networks, which visually represent relationships. Out of the two, matrices are particularly applicable for the current approach towards meaning generation from semi-structured interview data, as they can be used alongside thematic/content analysis to explore the interactions and conflicts described by the interview data with complementary effect. (Willig 2014)

This complementary use of thematic analysis and a matrix display strategy present the opportunity of exploring interactions amongst interview data on the topics of enquiry amongst the embedded units of analysis/participants clusters. By analysing the narrative at the intersection of the various descriptions and viewpoints, while supporting it with context data, the case questions can be addressed in a substantive, non-reductive manner. Additionally, the propositions, which come in the form of both the topics of enquiry and the stratification of the case, form a structural backbone for the interpretation and analysis of the data. However, they are also potentially challenged by the enquiry itself, based on the responses of participants across the groups. As a result, this procedural approach ensures that the data, the case questions and the propositions are inextricably linked in the process of meaning generation. Furthermore, the case structure is flexible enough to accommodate perspective plurality, meaning that conflicts between data points are descriptively meaningful, and their nature is a source of insight, rather than an imperative for interpretive reconciliation. (Miles *et al.* 2014)

3.3.3.5 Considering Methodological Validity and Validation

The notion of 'validity' within the context of methodology is a heterogenous, contested construct, largely driven by the philosophical framing of the study. Subsequently, the assumptions of critical realism shape the present contextual interpretation of validity and are largely based on both epistemological considerations and on the defined role of empirical observations. From a critical realist perspective, Zachariadis *et al.* (2013) notes that Internal Validity addresses the link between postulated mechanisms and the events which are observed and form the subject of data collection. Ensuring that such a link is adequately represented has been a passive theme throughout method selection and design. More specifically, it is addressed by the research strategy in the following dimensions:

- Case Selection: In addition to pragmatic concerns, the case selection criteria have been constructed to minimise the effect of circumstance/contingency on the manifestation of the postulated mechanisms.
- Data Selection: All secondary data sources are externally pre-validated and used with complementary effect to provide a nuanced picture of the operational context. Furthermore, the participant selection was conducted to ensure an adequate representation of perspectives and narratives based on the functional spread of the research problem (further elaborated in the following sub-chapter).
- Data Collection: In order to mitigate against researcher projection, measures have been taken to maintain data-collection nuance and represent diverging perspectives. Thus, interview questions are structured around topics rather than specific construct interpretations and aim to capture both perspectives and events. Also, by ensuring that questions across units of analysis are structured around the same core topics of enquiry, the potentiality of conflicting/diverging data is maintained.
- Structural Logic: Case findings are presented in relation to postulated mechanisms which, following the case-study, are readjusted and used to calibrate the problem-logic as the basis of prescription.

External Validity is used to describe the degree of generalisability exhibited by the outputs of the study. So, within a critical realist paradigm, it addresses the extent to which the mechanisms underpinning events in the setting of observation are also likely to be linked to events in different domains of application. That is why Zachariadis *et al.* (2013:7) suggests that "the degree of external validity is subject to discerning between the contingent factors from the necessary ones". In light of this, in an attempt to maximise external validity, emphasis has been placed on in-case perspective triangulation and context depth as a mean to develop a multi-granular, vertical/hierarchical, cross-functional interpretation of the in-case data to support the process of retroduction. By providing an in-depth overview of the functional, organisational, and sector context of the data, contingency and locality can be better accounted for when discussing the relationship between mechanisms and events. Whenever possible, comparisons are also made to highlight the effects of differences in context. Finally, the interaction between the theory-based postulated mechanisms and the in-case data is explicitly addressed in a standalone section (5.1) which aims to calibrate the

assumptions under which the process of prescription development can take place.

From a prescriptive output perspective (also covered in section 5), the notion of validity is largely inferred from the cumulative research narrative. In this context, framework design is seen as a process which leverages the foundation of theoretical and empirical findings to formulate a problem-specific adaptive pathway navigational archetype. In other words, prescriptive validity is approached as an extension of explanatory/representational validity. At the high level of abstraction entailed by the prescriptive contribution, the heuristic nature of constructs is predicated on axiomatic principles and assumptions. By emphasising the internal coherence and external applicability of these principles and assumptions, prescriptive contributions can be effectively formulated, assuming a better fit to the problem dynamics they address, i.e. organisational cybersecurity.

In addition, the inherently pragmatic nature of the prescriptive contribution, which shapes the interpretation of validity in favour of comparative or absolute performance measures, also positions the post-formulation validation outside of the boundaries of the thesis. This is due to the fact that subjective validation, i.e. the formal approval of stakeholders, is incompatible with the mechanism-based logic of the research strategy. The case has a moderating role for postulated mechanisms, and is not the sole manifestation of the research problem, which means that the problem addressed by the contribution is not bound to the case setting. In addition, the empirical data strategy converges a plurality of potentially conflicting perspectives under the conceptual arch-structure to yield findings, which excludes a monolithic representation of stakeholders/participants as vectors of prescriptive validity. Moreover, objective post-formulation validation presents a wide range of operational barriers, ranging from the ability to distinguish performance between the proposed prescriptive archetype and a baseline alternative; the inability to identify test-settings that are willing to implement the prescriptive output and accurately communicate measures of performance; and, the absence of an approach to normalise cyber security event contingency (defensive and offensive). As a result, both the added value and the practicality of constructing a post-formulation validation strategy for the study's prescriptive outputs are deemed insufficient.

To summarise, the single, vertically embedded case study was introduced as both an adequate approach for the empirical dimension of the project based on the research philosophy and objectives, as well as a pragmatic one. The issue of case design was also explored as a function of research questions, propositions, units of analysis, data definition, the link between data and the study's propositions, and the approach for interpreting findings. The following section will explore a descriptive and procedural outline of the data collection, management, and analysis processes which yielded the final case study.

3.4 Data Evaluation: A Procedural Outline

3.4.1 Engaging the Case

Prior to contacting participants, a series of procedural steps were taken. First, the premises put forward by the research design were used to develop supporting documentation. This includes: a Participant Information Sheet (Appendix 1), which provides a brief overview of the project, and is designed to accompany data collection/interview requests; a Consent Form Template (Appendix 2), whereby interviewees can explicitly review the potential uses for the data, and provide consent for the data capture method; and, an initial set of interview questions (Appendix 3), coupled with a rationale for enquiry, which are derived from the topics of enquiry in a group specific manner. Together, these documents were used to support a successful application for institutional Research Ethics approval.

As a central point of operationalising the research strategy, the interview questions are predicated on the assumption that the topics, which reflect the logic of enquiry (section 3.2), are linked to the core mechanisms underpinning the research objectives. Also, it is assumed that each topic is expressed/manifested differently based on the participant perspective and context. Thus, the initial questions were derived from the intersection of the topic of enquiry and the associated sub-constructs of the conceptual framework, with the broad attributes of the participant role clustering, in categories based on the functional division of cybersecurity management described in the previous chapter. Furthermore, the questions are seen as a point of departure, as adjusting the line of enquiry to reflect the specific insight of each participant is part of the research strategy. So, while the interview rationales remained constant for each group throughout the process of data collection, the questions themselves, as well as the emphasis placed on each section, were adapted throughout the process based on accumulating experiences, emerging opportunities, and participant responsiveness. The flexibility of the format was used to leverage a conversational dynamic for follow-up or elaboration requests on emerging themes. This flexibility was also used to de-emphasise group-based questions which seemed inapplicable for specific informants. Finally, driving the interview question formulation is the assumption that the link between relevant, empirical events and their underpinning mechanisms can be explored through a convergent narrative,

structured around the topics derived from the conceptual framework (described at different levels of granularity in sections 2.4 and 3.2);

Unlike the primary data, the mix of quantitative and qualitative secondary context data was collected both before case-selection, in order to ensure that the case meets the key selection criteria outlined in the previous chapter, and throughout the data collection stage, to follow-up and clarify emerging issues. The available quantitative data was used to provide a descriptive account of the context, developing a profile for University X in relation to both its sector, and the broader economy. This profile was then used to anchor open threat data and to support inference by appropriately positioning the case, while also establishing areas of possible contingency. The reliance on quantitative open data-sets and available descriptions of University X meant that representational detail can compromise anonymity efforts. Thus, efforts were made to ensure that sufficient context data is provided without compromising the identity of the case. Examples of such efforts include computing and describing economic performance in comparative rather than absolute terms, i.e. percentiles, or year on year performance compared to the sector average. As the sources and procedures used are described within the context development section (section 4.1), the remainder of this chapter is largely focused on the primary, qualitative data collection process and its subsequent analysis.

Given the low degree of structural transparency presented by University X's cybersecurity function, the interview questions have had to be adapted based on the emerging background of each participant. One notable point of departure from Brinkmann's (2013:21) overview of semi-structured interview practice consists of the inclusion of both descriptive and analytical/theoretical accounts as meaningful. While always discussed in a practical and local setting to the participant, the construct framing used by participants to conceptualise and describe occurrences is also captured by the questions. This also enables a better understanding of divergent data, particularly on abstract topics of enquiry where informant-specific understanding and framing can shape responses. In this context, both analytical and descriptive themes are deemed potentially valuable as enablers of representational consistency between the theoretical/abstract intuitive framing and practice.

A practical example of this necessity is presented by the critical representation of risk

constructs. Not only is a descriptive account of risk practices essential for addressing this avenue of enquiry, but the context, personal expectations, and their consistency with outcomes are also important to acknowledge. By exploring how the constructs are both understood and implemented from a plurality of perspectives, the congruence between the two accounts can be examined. So, while a descriptive account of events, evidence, processes and structures is indeed at the foundation of the case, some descriptive illustrations rely on theoretical/analytical interpretations, which make construct clarity valuable for narrative convergence.

3.4.2 Data Collection and Management Overview

The interview data has been collected over a period of three months, between the 25th of April and 27th of July 2017, and encompasses 11 interviews with an average duration of approximately 40 minutes. However, duration is not constant across groups. For example, Interviews with Group 3 'Operational Actors' were overall shorter, with an average duration of approximately 25 minutes, while Groups 1 and 2 interviews are correspondingly longer. All participants were sequentially contacted through e-mail — a process which has largely proven to be efficient, yielding mostly positive responses and further recommendations of individuals that were relevant to the study. Logistically, ten interviews took place on the premises of the institution, while the eleventh was conducted through VoIP. The organisational support of the study has enabled its logistical accommodation, which helped mitigate against logistical constraints. The most significant such constraint was presented by the limited time availability of some participants. This, however, has not compromised any of the interviews, as all the core topics have been covered in each instance.

One of the main challenges in implementing the research strategy has been the identification of a candidate pool that is diverse, relevant, and able to exhaustively address the research topics without over/under representing specific viewpoints. Given the low degree of visibility concerning University X's structure, and the specific qualifiers for each group, no a priori participant targets were set (Sim *et al.* 2018). A key part of gathering descriptive accounts of the processes and rationales behind in-case cybersecurity efforts and

conceptualisations was ensuring that informants have sufficient exposure and awareness to be able to accurately reflect the in-case reality. But this emphasis on interviewee exposure and awareness has yielded a series of additional aspects to consider. Firstly, for key strategic roles, even within a large institution, the pool of potential participants is very limited, which constricts choice — an issue further amplified by candidate availability and willingness to take part in the study. An in-case example of this issue lies with 'Category 2 - Cyber Risk Analysis' actors; after gathering a structural understanding of the case and its CS/IS risk analysis function, only three potential Category 2 actors were identified. This created a situation with very little room for error, as an understanding of this function is essential for outlining the case (the structure and role of in-case risk analysis will be further discussed in the following sections).

Secondly, by only selecting candidates based on their cybersecurity exposure and awareness, there is a risk of skewing the data based on specific areas expertise, at the expense of alternative views. This issue has been anticipated at the research design stage, and has been mitigated against through the interview categories. Whenever possible — most notably within 'Category 3 - General Actors' — efforts have been made to include a variety of perspectives, ranging from Academics (includes teaching and research responsibilities), Pedagogical Support Actors, Research Admin Staff, to Technical Staff (IT Development and System Maintenance), and Decision Makers — from different parts (I.e. Schools/Departments) of the organisation, with different backgrounds and levels of experience within University X. This varied pool of potential candidates is contrasted with that of key decision makers, or niche-expertise roles, where the scope of candidate selection variation is little to none — which can also inhibit the efficacy of anonymisation efforts (Saunders et al. 2014).

Keeping a balanced pool of candidates has also been difficult, given the lack of proportionality between the categories. General actors greatly outnumber decision-makers and risk analysts, however the addition of indefinite participants within the category changes the nature of the data-set in a way that does not address the primary case objectives, and provides little insight regarding postulated mechanisms. As the specifics of the organisational structure are largely externally opaque, a key step was identifying key informants and

establishing how to progress the candidate selection strategy. This has entailed a mix of Criterion and Snowball sampling approaches (Patton 1990). More specifically, once key informants were identified based on their organisational function, the subsequent interviews presented opportunities for additional insight into other roles of interest, and potentially valuable perspectives. This has meant that, while participation was constrained by a fixed, a priori set of criteria (i.e. adherence to the Group division), the perspectives of collaborators and the accumulating understanding of the operational environment have both influenced the ongoing candidate selection.

Stakeholder feedback indicated a necessity for the inclusion of an extended enterprise perspective to delineate and contextualise the case data. This was addressed through the inputs of a Cybersecurity-oriented informant from a sector oversight body within University X's extended enterprise, and that of a senior IT decision-maker within one of University X's commercial spin-offs. The former enabled capturing a perspective informed by a wide exposure sector-wide cybersecurity, while the latter helped gain an understanding of the role and relationship between University X and its commercial spin-offs, especially in relation to cybersecurity. Both perspectives played an important role in better understanding the dynamics, the context, and the contingencies of the case. Finally, the phrasing of questions and the specific areas of emphasis have also evolved throughout the three months of data collection based on perceived effectiveness. After each interview, the notes and recordings were reviewed and evaluated for preliminary themes and interview practice efficacy. The findings were then used to inform the following interviews.

3.4.2.1 Describing the (Anonymous) Case and Participants

Given the potential sensitive nature of the research area, anonymity for interviewees has been explicitly included within the research design to stimulate participation and ensure that both individuals as well as the institution do not face repercussions because of the study. However, Saunders et al. (2014:617) present the pursuit of complete anonymity within qualitative studies as an "unachievable goal" and, instead, highlight the need for a "balancing act" between protecting the identities of participants and preserving the data's integrity and value. The most notable example of this tension within the current project lies with the

description of roles and professional background of participants. Both attributes were used for interviewee selection and are meaningful for accounting for the context of the interview data. However, overt descriptions of roles and backgrounds raise the issue of potentially compromising participant anonymity in relation to other actors within the research setting.

Several measures are taken to balance the two objectives. Pseudonyms in the form of gender-neutral names have been randomly assigned to each candidate. The individual pseudonyms are extracted from an online database of such names. The resulting list of names is also culturally standardised, as both participant personal background and gender are irrelevant for the object of study. Furthermore, gender pronouns are avoided in favour of the third-person, singular "they". If individual quotes are perceived as sensitive, attribution is made based on respondent group, I.e. "Member of Group 3 - General Actors". It should also be noted at this stage that, within the context of data analysis, a broadly 'empathic' interpretative stance is taken, as the nature of the enquiry does not rely on assumptions of implicit meaning and motives outside of the statements of participants (Willig 2014). Nonetheless, inferences are made from the comparison of individual statements, whenever adequate, to account for plurality of perspectives, inconsistencies, and ensure that nuance is adequately represented.

However, not all personal attributes have been suppressed. To maintain the value of the collected data and provide adequate context, relevant individual characteristics are presented. Examples of this include the time spent in the organisation where this is seen as contextually relevant (adjusted/approximated so that it is not a direct identifier), or, when explicitly stated, broad descriptions of background and experience which inform various positions. As a rule of thumb, such attributes are made explicit when they are essential towards understanding the context of the data. The full list of interviewees, their assigned pseudonyms (used throughout section 4.2), and their descriptions/profiles have been included in Table 2.

Pseudonym	Group	Description	Notes
Charlie	1	Mid-management role, with direct input over technological behaviour. Non-academic; Feeds into senior management; Role entails wide exposure within the organisational structure;	• >3 Years in Institution; • Management Role for Secondary Technology Infrastructure; • "Feeds into Senior Management" – Outside of traditional Hierarchy; • Wide exposure and oversight, as the role covers multiple 'schools'
Val	1	Part of leadership team; Organisational growth-oriented role; Substantial background experience relating to cybersecurity.	• Senior role grounded in growth and innovation • Additional policy, advisory and entrepreneurial experience within cybersecurity. • Meta-departmental/functional
Alex	1	ICT Senior Management Role; Direct decision-making responsibility; insight into the IT function's approach to Risk	• CTO equivalent – role emphasis on ICT/Technology and Strategy. • Oversight of ICT technical programmes, development and strategy. • Operational perspective on cybersecurity and risk analysis
Ash	1	Senior Management role in ICT for Subsidiary; Decision-making function within the technical facets of the Subsidiary	• Senior Managerial ICT within 'for-profit'/ventures institutional subsidiary. • Role entails decision-making and strategy development for the technical dimension of operations
Brooklyn	1*	Cybersecurity Management Role in Industry Oversight Organisation; Broad exposure to sector issues; Access to a wide variety of institutions.	• Management role in Cybersecurity; • Part of an industry body with cybersecurity responsibilities and oversight; • High levels of exposure to sector-wide trends and patterns; • Macro compliance expertise.
Rudy	2	Information Security Management and Risk Role' Direct engagement with the risk analysis process; Feeds into decision makers/senior management; Meaningful professional background	• Responsible for formal IS Risk Analysis; • Directly feeds into policy and senior management; • Varied technical/managerial background outside of the sector.
Eli	3	Academic role within School A; Significant experience within the institution (~10 years); Daily tasks fully dependent on ICT infrastructure;	• Operational role: teaching and research in Faculty A. Above average seniority (given staff turnover): exposure to restructuring/ • Representative in day-to-day role and tasks
Kendall	3	Non-academic role; Involved in research/project management and support. >20 years of institutional experience in various roles (including technical); Direct exposure to high value data.	• Administration, project management, and research support role; • Exposure to externally opaque projects, research and data; • Previous technical/managerial background;

Remy	3	Core Technology Development/Support role; Oversight and management of core (pedagogical) systems.	• Core technical support actor • Oversight of operations for operationally vital technologies (i.e. VLE) • Dual perspective, exposure to and familiarity with aggregate user behaviour
Sage	3	Non-academic dual role: staff training and technology support; Academic research background.	• Responsibilities include learning technology support, staff-oriented workshops. Research adjacent. • Role entails engagement with both operational actors and senior management
Fin	3	Academic role within School B; Significant international experience	• <3 years in current role • Role entails a mix of research, teaching and admin tasks representative of School B; • Cultural point of reference, given international previous academic experience.

Table 2. Participants overview and selection rationale

Finally, despite its flexibility, the participant clustering described as part of the research strategy has been, in practice, less than obvious. So, for example, 'Alex' as a Senior Manager/Leader within the organisation's IT function, could have addressed both 'Group 1 - Decision Makers', and 'Group 2 - Risk Analysis' perspectives. As this categorisation impacts the set of questions that guide the interview, adequate categorisation is important to maximise the value of the data. In such instances, a judgement call was made based on the individual participant exposure and oversight, the primary function of their role, and the distinctness of their perspective. So, in such instances, the scope of the conversation was broadened beyond the Group-based questions in order to maximise the insight gained from such candidates. As this limitation of the Group clustering became apparent within the first interviews, the mitigative steps were designed early in the process, leaving room for 'opportunity questions' and narrative variation, at the expense of a strict adhesion to the question sets.

3.4.2.2 Mitigating Data Collection Bias

While efforts to mitigate against researcher bias have been made implicitly throughout the development and implementation of the research strategy — most notably with respect to

internal validity — they have also played an explicit role in engaging the case. Miles *et al.* (2014) address the issue of analytical bias from two perspectives/origins: the influence of the site, i.e. case, on the researcher, and vice versa. Examples of explicit steps taken to address these can be loosely clustered around:

- *participant selection*: the participant spread was maximised, where possible, to potentially reflect status/perspective divergences (such divergences are reflected in the interview data); the informants' duration spent in the organisation was used to identify opportunities for capturing historical context, including cultural and procedural background dynamics which contrast the status-quo; in order to maximise transparency, all participants were briefed about the objectives and the rationale of the study prior to data collection;
- *engaging the case*: the data collection architecture entailed triangulating perspectives on the key topics of enquiry; external (secondary) sources of information where also used when available, most notably to frame the organisational context; the interviews were anchored in the core constructs and research objectives, which provide a conceptual point of convergence for the research narrative; obtrusive observations and measures were avoided in order to ensure a collaborative dynamic; ongoing feedback was sought from the doctoral supervisory team as a source of procedural calibration and objective/third-party input;
- *subjective/behavioural measures*: internally conflicting viewpoints (i.e. conflicting accounts from the same participant) were used as indicators of potentially 'loaded' question framing, explicitly noted in the preliminary data analysis, and used to adjust follow-ups; even when sought by participants, potentially biasing researcher inputs on the research narrative and objects were postponed until after the interviews; finally, given the contextual logic of empirical enquiry and the coarse granularity of the postulated mechanisms, there were no embedded incentives to favour specific findings at the expense of representational accuracy.

3.4.3 Data Management and Analysis

Interview data analysis is broadly described by Roulston (2014) as a three-stage process: data reduction, data reorganisation, and data representation. Within the current study, the first stage corresponds to interview data processing and coding. The second step entails exploring for patterns connections within the data — achieved through a matrix display (Miles *et al.* 2014). Finally, these patterns are explored fully and represented within the case narrative. It is also worth noting that, in addition to the formal analysis process, a preliminary analysis of the emerging data was conducted in parallel to the collection process, as proposed by Miles *et al.* (2014). This preliminary analysis was cyclical and ongoing throughout the duration of the data collection stage, and it was primarily used to refine the questions and assess converging insights in relation to their potential for case-building. From it, a series of relevant aspects have emerged, which have included the necessity of incorporating an organisational commercial spin-off point of view, the opportunity for greater context insight provided by sector-level oversight actors, and the perception of structural data saturation which triggered the progression of the study.

3.4.3.1 Interview Data: Transcription and Management

Prior to the formal analysis stage, the data was first prepared in alignment with the research assumptions and strategy (Roulston 2014). Following the interviews, the audio recordings were manually transcribed in their entirety. This process was software assisted, which enabled Duration/Location coding for time-tagging text to its corresponding position in the audio recording. In addition, due to software time-stretching and dynamic navigational shortcuts, as well as high fidelity recordings captured in largely controlled environments, the process of capturing audio-content has been generally unhindered by unintelligible/unclear recordings. Furthermore, as the transcription was not outsourced, potential interpretational disparities were also mitigated through the recollection of the interview narrative and notes, as well as the researcher familiarity with the source material. A ‘Standard Orthography’ (Kowal and O’Connell 2014) representational approach was used, meaning that no emphasis was placed on preserving dialects or phonetical variations. However, when deemed meaningful,

paralinguistic components such as laughter or tone (i.e. indicating sarcasm) were highlighted and captured as an annotation to ensure that the context of individual statements is not lost. Finally, preliminary anonymisation measures were also taken in the transcription process, which primarily consisted of replacing key names or unique identifying attributes with codes. (Kowal and O'Connell 2014)

When not in use, both the notes and transcripts were password protected and stored on 256AES encrypted drives. Transitioning towards the qualitative data analysis stage entailed importing all relevant text files into NVivo, where they were preliminarily processed through meta-data generation, ensuring transcript format consistency, and general data cleansing.

3.4.3.2 Coding Interview Data: Reduction

The coding approach used for the data reduction stage is based on Miles *et al.* (2014), who describe the practice as labelling data segments based on both their meaning, and on their broader epistemic attributes. This approach is centred around two cycles, the first of which aims to assist with categorising the data, while the second is used to reorganise it in order to yield patterns.

As a result, after the appropriate meta-data was produced, a preliminary coding structure was established. At this stage, ongoing engagement with the interview data was a key step in establishing and reiterating on codes and themes. From this process, five distinct types of codes emerged. This categorisation relies on the wider spectrum of coding approaches introduced by Miles *et al.* (2014). Individual codes contain their category embedded as a prefix, followed by their corresponding topic, and, when appropriate, an additional qualifier. The prefixes and their corresponding categories are:

Des. — Descriptive Coding: includes procedures, circumstances, events and outcomes;

Em. — Emotion Coding: identifies affective statements, attitudes, trust, and intuitions;

Hol. — Holistic Coding: describes macro themes, and generally covers larger sections of text;

IV. — In Vivo Coding: code reflects direct phrasing of participant

Hyp. — Hypothesis Coding: a largely secondary code encompassing statements relating

to the Knowledge Problem heuristic.

Throughout the second cycle, codes were bundled where possible based on themes, explanatory content, or the underpinning construct they address. A practical example of the ouptut of this process is: “des.Anecdotal Evidence_Computing Behaviour”. This code was used to identify the sections of interviews where participants anecdotally describe occurrences related to their computing behaviour. ‘Computing Behaviour’ is one of four categories of anecdotal evidence descriptions identified. Following a reiteration process in which unnecessary codes were collapsed or converged, a total of 68 codes remained, 49 of which being categorised as descriptive. Each of the codes was individually defined, while some were hierarchically organised based on their topic and content commonalities. Following this stage, the data was reorganised in the form of a matrix display, as an extension of the reorganisation role prescribed for Second Cycle coding. Matrix displays are described by Miles *et al.* (2014:108) as a “…tabular format that collects and arranges data for easy viewing in one place, permits detailed analysis, and sets the stage for later cross-case analysis ….”.

3.4.3.3 Representing Connections: Themes and Patterns

The purpose of the matrix representation was to restructure the heterogeneous interview content from across the participant groups/embedded units of analysis to connect the findings around the case questions and topics of enquiry, and enable their convergence into a case narrative. It was also used as a final filter against interview content which does not support achieving the research objectives while at the same time further reducing the volume of the insight gained. As the case questions were not designed to yield a simple truth-claim answer format, the need to capture the dynamics, layers and potential mechanisms driving the research topics for case building placed substantial emphasis on structural clarity.

These requirements are reflected in the adopted structure. The headers used are: ‘Case Question/Objective’; the respective ‘Sub-objective’, which is derived from the Logic/Topics of Enquiry, and enables a systematic deconstruction of each primary objective into segments; the ‘Theme’, derived from the coding cycles; ‘Interview Identifier’ for each participant; relevant ‘Quotes’ and data excerpts; ‘Point’, which encompasses a quote summary and

categorisation as either descriptive or analytic; 'Notes' for each point made and its non-local implications from a narrative standpoint; and 'General Notes' used to summarise cross-group patterns at a theme level. Furthermore, the theme level summaries captured in the 'General Notes' column were also colour coded based on their relevance towards the emerging narrative. Table 3 exemplifies 3 (randomly selected) nodes out of the 114 included in the matrix representation of the data. It thus serves as an illustration of the analytical process used to connect and represent themes and patterns. A more in-depth overview of the structure and contents of the matrix display as outputs of the reorganisation stage of analysis (Roulston 2014) is introduced in Appendix 6. This provides a clearer picture of the analysis process, and further illustrates the transition between the raw interview transcripts and the case narrative as a function of data and pattern analysis.

Macro-objective	Identify how knowledge relating to cybersecurity is produced, used and adapted at various levels within an organisation
Sub-objective	Role of KNW
Theme	(des).Uncertainty in CS
Interviewee	*Participant* GR1
Quote	I think it is speed. Speed of impact, I think, with cyber. Lots of the other uncertainty, around government changes, around Brexit… it's a much longer lead time. You've got some planning, you can put plan a, plan b, plan c, and you can make representations, you can lobby, you can build the networks. Cybersecurity - it's there when you're dealing with it. Or cyber-attacks. So, yeah speed. #00:39:23.99# Speed is the definite thing. And also, I suppose, the breadth of impact. #00:39:31.81#
Point (Des – An)	AN: Uncertainty in CS is Distinct due to Speed and Breadth of impact
Notes (Entry)	Pace and Breadth of impact (variance): Ties in Knowledge with Change as Topics. Also consistent with risk/systems theory assertions concerning the role of risk in high uncertainty.
Aggregate Notes* (Theme)	Uncertainty in CS distinct due to: Speed and breadth of impact, scope of 'Unknown unknowns', and their impact, and consequence of unpredictability

Table 3. Example A) 1 out of 5 entries for "des.Uncertainty_in_CS" Node; *Aggregate Notes reflect all entries in a Theme;

Macro-objective	Identify how knowledge relating to cybersecurity is produced, used and adapted at various levels within an organisation
Sub-objective	How KNW is Validated
Theme	(des).Knowledge in CS_Validity
Interviewee	*Participant* GR1
Quote	But I think… the thing is, it's almost a bit of learn by doing. You're going to have a few false positives initially, or things that you miss. And as you get more experienced, you learn the things that you really have to take notice of. It's almost back to that conversation we've talked about training the machine intelligence - it's that same process. So yeah, you do have to

	validate it. Again, an external company can help with that cause it just gives you a different set of eyes. Our internal people, our ethical hacking students, again - that's where they're quite useful for, cause they're coming at it with no preconception, you know? #00:24:15.20# [...] So, be outward facing and be unafraid as an (ICT function) to accept that what can be perceived as criticism. Nobody is doing this perfectly. And what people will appreciate is that you're doing your best, you're communicating, bringing people in, and you learn, by doing in essence. By partners - the HE community is quite good in the IT space, they're talking to each other. #00:25:04.99#
Point (Des – An)	AN: Knowledge validation - An adaptive iterative process built on feedback. External feedback is encouraged.
Notes (Entry)	Process outline: The structure of the process of validation is described, as iterative, collaborative and bias-mitigative through the involvement of a 'different set of eyes'. Emphasis on empirical testing/feedback, communication, adaptation and iteration.
Aggregate Notes* (Theme)	Value of knowledge validation is undisputed amongst the interviewees. Methods for validating knowledge include: consideration for temporality and contextuality, iteration and collaboration with external entities, empirical testing, trust in source;

Table 3. Example B) 1 out of 4 entries for "des.Knowledge_in_CS:Validity" Node; *Aggregate Notes reflect all entries in a Theme;

Macro-objective	Critically analyse the role and epistemic requirements of CRM
Sub-objective	Cyber Risk and the Knowledge Problem
Theme	(des).Awareness_and_Communication
Interviewee	*Participant* GR2
Quote	The university has its sets of policies that are not known to everyone. […]- It's difficult… No one wants to be involved in a breach. And, in the security health check visits we've made people are very very keen to speak to us. But first they're often quite nervous. They think this is going to be some sort of grilling, it's going to be an audit. No - we're here to help, we're here to advise. If we find a problem, we're not going to point a finger, we're going to help you to mitigate it. And it's very difficult - people have got their day job. They're very very busy, and sometimes security isn't top of mind, and they'll do something quick and not realise it's dangerous. So this is very very hard, to try and instil this culture of security. #00:35:42.29#
Point (Des – An)	DES: Policies are not known to everyone; AN: 'No one wants to be involved in a breach' DES: people 'very busy' - ' security isn't top of mind'; DES: Very hard to instil a culture of security
Notes (Entry)	Procedural opaqueness seems to be a reoccurring theme. Pockets of knowledge and awareness prevent more effective user defensive behaviour, and also bypass IT and [Information Security Function] 'radars'
Aggregate Notes* (Theme)	Policies not known to everyone. High value of feedback obtained through informal means; 'ICT Risk' must be translated to business speak; Breaches occur in spite of intent, not because of it; Anecdotal evidence of staff interest in technological safety (*GR3 Participant Link); Organisational size means that 'it —communication — depends on process'; Asymmetry in staff capabilities (*GR1 Participant Link) and awareness; Posture depends on member of staff (technical or managerial); Actor awareness and self-evaluation ability seem limited; Limited threat awareness - bottleneck; Education deficit perceived

Table 3. Example C) 1 out of 11 entries for "des.Awareness_and_Communication" Node; *'Aggregate Notes' reflect all entries in a Theme;

In its totality, the resulting structure can be described as a meta-matrix which enables multiple levels of representational granularity, ranging from the broad case question, down to individual quotes and their contextual implications. It also provides structural clarity concerning the link between the filtered data and its relationship to the wider case questions. In addition, it enables a relational understanding of the connections amongst themes across the embedded units of analysis, and of the ways in which these impact the principal objectives. The resulting insights were converted to a case format — the final form of the study's empirical output (Section 4.2). However, the process of representing and structuring the case in the form of a narrative is a function of the preceding stages of data analysis. While the case-study aims to preserve and maximise the insight generated from the data, to reduce its volume, and to maximise coherence, its reliance on the matrix display is manifested structurally, and is paramount for ensuring narrative fidelity and representational nuance. A word-cloud visualisation of the interview transcripts was also included in fig. 3.

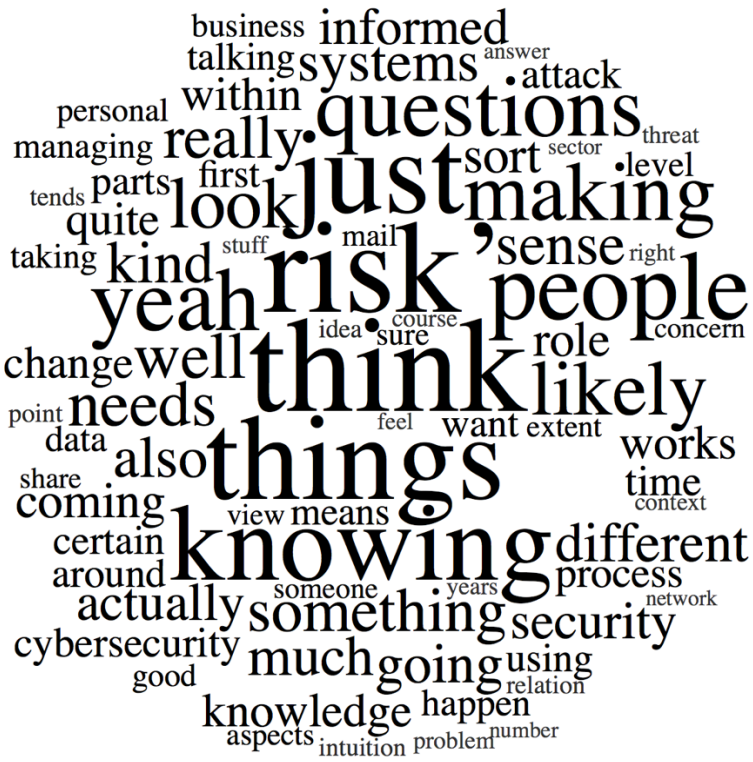


Fig 3. Word-cloud visualisation of interview transcripts

4. Case Study

The case study section serves as the final output of both the primary and secondary data collection and analysis processes, and is the principal empirical contribution of the research strategy. It aims to provide a hierarchical, cross-functional perspective of the dynamics between cybersecurity, knowledge and risk in an exemplary setting. In order to achieve this aim, it is structured in two different sub-chapters. The first employs a variety of secondary data sources in order profile and position the case, University X, in its operational context, while also illustrating the attributes of said context. The second sub-chapter consists of the case narrative itself, and is primarily structured around the two research objectives which it aims to address. The case text explores the various perspectives captured through descriptions and direct quotes, while also providing commentary on how these affect the conceptual picture built by the preceding theoretical analysis, in relation to the overall organisational context. In its conclusion, the case study attempts to summarise the emerging findings in anticipation of the framework development section.

4.1 Case Context: Sector Outline

The research strategy built throughout the previous sections emphasises the role of ontological mechanisms manifested across systemic layers in understanding the dynamics of an applied phenomenon like cybersecurity. As a result, the context of the case in relation to the sector and the wider economy is important for considering contingency in empirical outputs. The following section will attempt to present the backdrop of the case data through a compilation of quantitative and qualitative secondary sources. These include government and third-party reports, industry open data sets, as well as research conducted by sector overview agencies. Through such sources, the wider relevance of the case, as well as the generality and, respectively, the locality of its attributes, structures, and events can be considered. However, this objective raises an important challenge: presenting detailed case-data without compromising anonymity. Subsequently, descriptors and indicators of performance will be presented in a comparative rather than a direct manner whenever these might directly affect the anonymity of the case.

The hybrid nature of the Higher Education sector within the UK entails a rare mix of transparency and accountability in financial activities beyond that of private enterprise. It exhibits economic integration, supported by incentives for monetisation and income generation that are uncharacteristic of other public-sector ventures. As a result, through non-profit bodies like HESA (2017), in-depth descriptive data is available, covering the precise scope of the sector in terms of its year-on-year financial performance, number and attributes of accredited active institutions, as well as metrics on the role these play in engaging and supporting communities, generating intellectual property, employment and education, research, and pursuing spin-off ventures. This context data provides a distinct opportunity to account for externalities in understanding the role and impact of individual cases beyond that of fully private ventures where performance and societal function is quantified in a primarily financial manner.

From a financial perspective, the sector-wide state of affairs is convoluted. Despite exhibiting a growth in total income of 31.3% between 2008-2009 and 2014-2015, which substantially exceeds the rate of inflation (CPI 16,2%) (Grant Thornton 2016), political turmoil and uncertainty are likely to impact future performance to an unknown extent. At the time of writing, the latest available sector-wide financial data covering 2015-2016 indicate a 3.6% increase in total income, and a 48.8% increase in net surplus when compared to the previous year. The overall sector income for 2015-2016 amounted to £34.739bn, with a total number of 163 universities represented by HESA within the year's data set. Within this context, the case — University X — significantly outperformed the year-on-year average income growth, as shown in fig. 4. University X is placed amongst the sector's top quartile regarding financial performance. The quartile-based division is also employed in the Grant Thornton (2016:9) report, highlighting a disproportional income growth trend for quartile one institutions when compared to the rest of the sector (10.0% Q1 vs. 1.5% Q4).

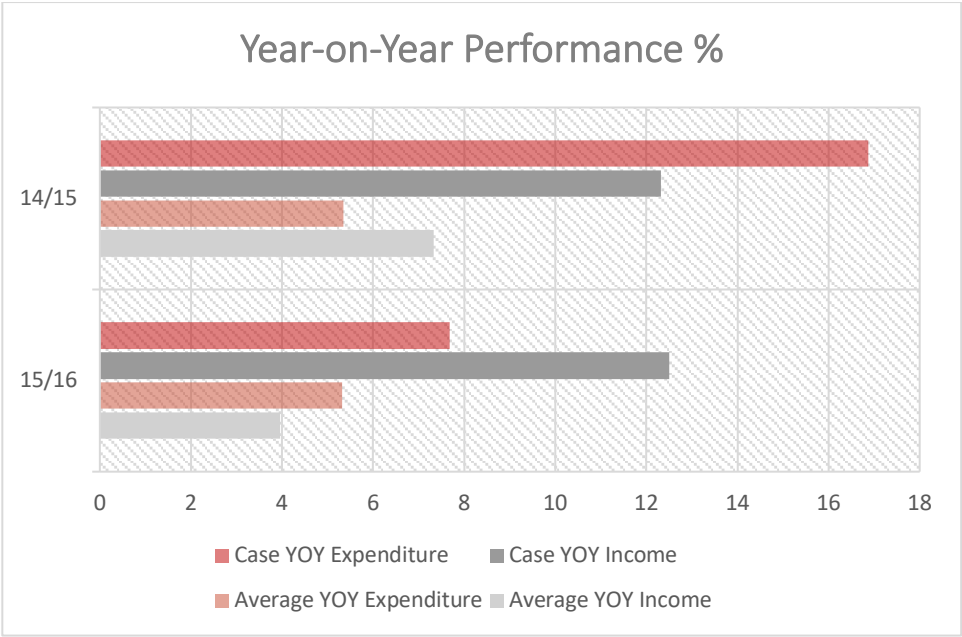


Fig 4. University X year-on-year % change in income and expenditure compared to the sector average (based on HESA 2017)

Staff and student numbers are tangentially relevant to sector and institutional cybersecurity as determinants of operational scale. Furthermore, institutions are owners of both staff and student data. Thus, an understanding of the sector average, total, and University X's relative actor footprint can help better outline the context, while enabling cross-sector comparisons with data from sources such as the yearly Cyber Security Breaches Survey (Klahr et al. 2017). At a sector level, HESA's (2017) 2015-2016 staff data-set indicates a total of 201380 Academic contracts, out of which 135015 are full time, 208750 non-academic contracts, and 72015 atypical contracts, accounting for 163 institutions. Based on its full-time staff footprint, University X is positioned in the top quartile. From a student perspective, the total population accounted for 2.28mn in 2015-2016, which indicates the first positive year on year change since 2010/2011 (fig 5.). Again, University X is positioned in the top 25% of UK universities based on total student numbers.

Fig 5. Total Student Number Dynamics (HESA 2017)

In addition to their direct economic footprint, higher education institutions also play a role in a range of spin-off companies which can exhibit varying degrees of institutional involvement and ownership. These include staff start-ups, graduate start-ups and social enterprises, which, in 2015-2016 employed 44335 people, almost half of which through graduate start-ups (22592) (HESA 2017). The total turnover of these companies amounted to £2.51bn for the year, a 4.89% decrease from the previous year's figures. In addition, the HESA data accounts for institutional contributions to economic development through a series of 'soft' criteria, including widening participation and access, supporting regional graduate retention, facilitating knowledge exchanges, supporting SMEs, encouraging student and graduate entrepreneurship, providing support through incubators, attracting inward regional investments, conducting research collaborations with industry, attracting non-local students to the region, supporting community development, establishing local partnerships, developing management, meeting regional and national skills needs, commercialisation, and network facilitation. Through self-evaluation, University X indicated activity in all the above, with emphasis on knowledge exchanges, SME support, and research-based collaborations with industry partners.

So, beyond their (significant) teaching and research activities, institutions within the Higher Education Sector can act as hubs within diverse networks of actors and value streams. Their

involvement in subsidiaries and spin-offs, technology transfer initiatives (HOC 2017), as well as various types of partnerships and services provided to industry, creates a highly complex environment from a cybersecurity perspective. More specifically, such institutions must defend a diverse, valuable and sensitive informational asset base, complex infrastructures and system designs, while also providing support for stakeholder dependencies — all valuable attributes when exploring cybersecurity as an applied phenomenon. In addition, infrastructural common denominators such as the JANET network, non-adversarial operating models, sector bodies, and comparatively high openness and transparency (as opposed to other knowledge intensive sectors) all underpin the potential explanatory value of the research context.

Institutions within the sector largely face two distinct sources of pressure to engage with cybersecurity: threat actor behaviour, and regulatory/legislative compliance. Before proceeding to the case-data, sector level context will be provided on each of these.

While the scope of the threat presence faced by the sector is hard to objectively gauge due to the general institutional reluctance to disclose security breaches, several proxy indicators can be gathered from secondary data. The JISC (2017) Cybersecurity Posture Survey indicates an increase in both the proportion of Higher Education institutions with a dedicated cybersecurity budget (excluding staffing) from 40% in 2015/2016, to a projected 58% for 2017-2018, and in the scope of the average budget. While not a measure of threat activity, this growth can indicate increasing concern and/or awareness from institutions. The 2016 VMware report on UK Higher Education cybersecurity provides additional survey data, on a sample of 75 respondents/50 universities, which suggests that 79% of responding universities had suffered reputational damage, 36% face hourly attacks, and 87% have been breached at least once.

These findings are comparable with data from the Cyber Security Breaches Survey (CSBS) (Klahr *et al.* 2017). The latter spans outside of the sector, and clusters responses based on organisational size, and broadly based on sector. According to the survey, 60% of 'Professional, scientific or technical firms', and 68% of Large firms have experienced a security breach or attack in the previous 12 months. It is worth noting that, according to HESA staffing data for

2015-2016, the vast majority of UK HE Institutions can be classified as 'Large firms', having over 250 employees. If using investment in cybersecurity as a proxy measure, the 2015/2016 yearly average budget of £374.250 for higher education institutions within the JISC (2017) data, and the 'Average investment in cybersecurity in [the] last financial year' (given the report publication date, assumed to be 2015/2016) for large firms within the CSBS, which amounts to £387.000, the classification of HE institutions using the 'Large Firms' data cluster seems adequate. However, despite a seeming consistent narrative, it is also important to emphasise that the degree of representativeness of universities as a sub-cluster of 'large' enterprises in terms of cybersecurity posture cannot be fully extrapolated from the available data.

Nonetheless, the survey (Klahr *et al.* 2017) also found a correlation between the occurrence of breaches and the existence of defensive efforts, as the clusters of respondents which have provided cybersecurity staff training, have made investments in defence, have implemented governance measures, or risk management efforts, all present a larger number of incidents than the total population. Potential explanations for this counterintuitive phenomenon include the possibility of more extensive defence efforts being more frequent in organisations which face comparatively high threat activity. However, the existence of such defensive efforts could also indicate a higher ability of identifying the occurrence of a breach. Similarly, the JISC (2017) survey finds Further Education respondents to be more confident in their cybersecurity posture (average score of 6.8) than Higher Education counterparts (5.8), in spite of having a significantly lower proportion of institutions with a dedicated budget (~23%), lower average budgets, and a lower presence of dedicated cybersecurity staff (72% HE vs 3% FE). From a case selection perspective, both potential explanations for this correlation favour a larger institution with a dedicated budget as a more adequate setting of enquiry.

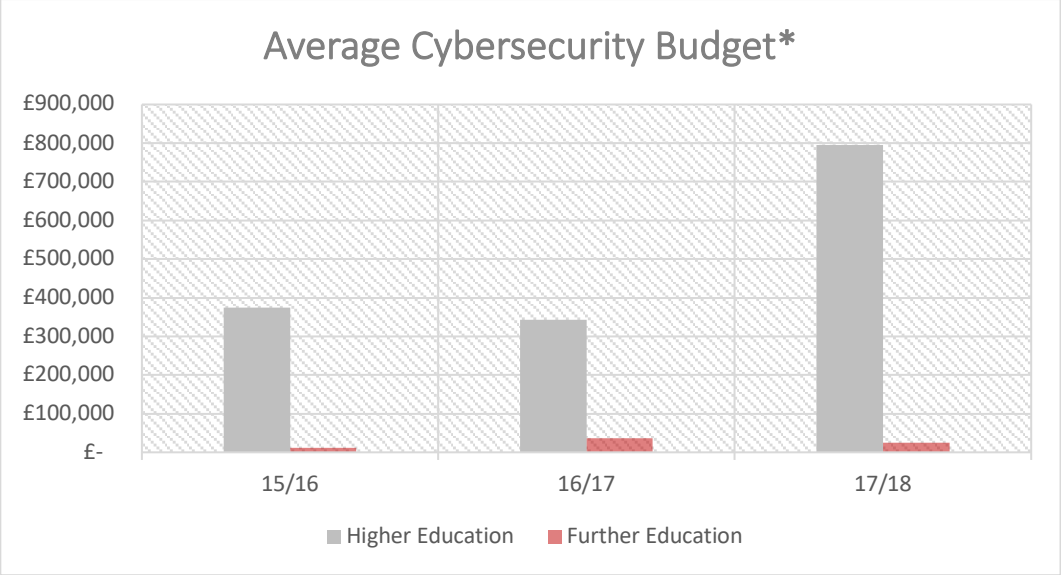


Fig 6. Average dedicated cybersecurity budgets, where 'known' (JISC 2017)

From a compliance perspective, UK Higher Education institutions do not, at the time of writing, face any sector-specific regulatory frameworks (Hogan Lovells 2016). However, the transition from the UK Data Protection Act of 1998 to the EU wide General Data Protection Regulation (ICO 2017) is a substantial step affecting all universities, due to their use of personal data. GDPR Compliance is identified as a top "cybersecurity area of importance" for both HE and FE institutions within the JISC (2017) Survey Data. The significant effects of this transition for HE institutions, and more specifically the case, have been highlighted within the interview data. Based on context and scope, the notion of compliance can also be applied in relation to stipulations of cyber insurance policies, institutional policy and strategy, as well as specific frameworks, standards and accreditations which are pursued. The most notable examples of the latter, as applicable to HE institutions are the UK Government's Cyber Essentials and Cyber Essentials Plus (GOV.UK 2018), as well as the ISO27001 Standard (ISO/IEC 2013). JISC (2017) data indicates that 20% of respondents have achieved the Cyber Essentials accreditation, while 38% are working towards it — a significant difference from the ISO/IEC 27001 Standard which was achieved by 3% of respondents, with 12% working towards it. It is also worth noting that this preference seems sector specific, as the CSBS (Klahr et al. 2017) data indicates significantly more 'large firm' institutional awareness concerning the ISO/IEC Standards (57%) versus the Cyber Essentials scheme (28%). A case-specific discussion of the applied nature of compliance efforts based on interview data will be covered in the case-

study.

So, to summarise, the UK Higher Education sector provides a unique opportunity of insight concerning cybersecurity in a knowledge-intensive environment. Beyond their wide variety of stakeholders, and broad involvement in a range of economic and social growth initiatives, HE institutions operate within accentuated dichotomies, most notably openness and security. Universities are also presented by the UK Government (2016) as part of its National Cyber Security Strategy 2016-2021 as creators and owners of intellectual property, partners to industry and government, as well as assets in addressing a cybersecurity skills shortage. An operational model heavily reliant on reputation and stakeholder confidence ensures strong incentives for breach avoidance. Finally, in spite of substantial expenditures, the sector operates under a surplus, with top performers (Q1) exhibiting substantial year-on-year growth. Thus, such institutions also possess the capital required to pursue changes which are deemed appropriate in relation to cybersecurity pressures. The importance of gaining a vertical understanding of the case data has been emphasised in accordance with the conceptual framework, which places a high importance on analytical scale granularity and context specificity in exploring an applied phenomenon.

4.2. Case Data

The exploration of the case data will be primarily centred around the first two research objectives: to develop a substantive understanding of how cybersecurity knowledge is understood, produced, used and adapted across hierarchical levels within an organisation; and, to critically explore the role and epistemic requirements of Cyber Risk Management efforts. The two objectives are complementary, and enable the pursuit of the third, prescriptive objective — to conceptualise a risk-based framework rooted in the knowledge-uncertainty dynamics that are characteristic of organisational cybersecurity. Beyond the two objectives that are directly anchored in the case-data, the interview topics also provide a common strand of narrative support and theme clustering, as will become apparent in the following. In spite of the seeming separation between the topics, they are deeply interwoven when examined in an applied setting. That is why, if structuring the case data around the research objectives, neither the topics nor the themes can be exclusively clustered to fit a single section. So, it is worth noting that the data and its contextual meaning are not inherently linear, as themes and topics are covered based on the narrative of the research objectives, which can lead to instances of repetition. It is also worth noting that overall narrative content, quotes and general conclusions are a product of the multi-stage data analysis sequence described in section 3.4 – most notably, the matrix display which is structurally exemplified in Table 3.

4.2.1 The Applied Dynamics of Cybersecurity Knowledge: University X

4.2.1.1 Context and Case Description

In order to discuss cybersecurity knowledge within the context of the case, the scope of cybersecurity as an area of interest for University X should first be established. Both academic and non-academic participants presented cybersecurity as a current concern within their roles. However, the nature and the extent of said concern varied significantly across interviews. For example, Eli, as an academic actor classifies cybersecurity (CS) as “a major concern” that is personally “very important”. More specifically, Eli recognises the disruptive potential of a breach for their ability to conduct their tasks: “*For me, I mean, almost all the*

work that I do [is] online. So, if anything should happen to that, it's like I've got nothing to do". In contrast, Kendal as a non-academic actor views cybersecurity as potentially concerning in relation to the "very sensitive data" used by his organisational function. However, this view tends to be abstract, due to an avoidance of ownership for such data: "*The sensitive data, I try not to get involved with. That is down to […] the person who is in charge of the research*".

The relationship between an active concern regarding potential breaches and the perception, or awareness of personal liability is also made apparent by Fin, who recognises the confidential nature of some of the data under their ownership, however views cybersecurity as a primarily institutional issue: "*I am not particularly bothered about it, in the sense that I think that while here, the institution takes care of many aspects. And I just take care of certain aspects that are related to myself particularly*". The primary criterion for this division is presented as the ownership of the hardware/infrastructure: actors should show vigilance ("*shouldn't […] open all sort of e-mails that are not trustworthy and so on*"), especially when working off personal devices ("*I also have a personal laptop, and I need to take care of that, naturally*"), while the institution should provide "*a safe environment*" consisting of "*secure servers and all the systems that we'll be using to share files, emails, etc.*"

As a leader/decision-maker, Val presents cybersecurity as an implicit aspect of their role, which, while not "*at the top of [the] list*" of priorities, has the potential of becoming a "*disabler*" for change and growth — both essential aspects of organisational performance and strategy. Similarly, from an IT Management perspective, Alex paints a nuanced picture of cybersecurity that is shaped by dichotomies. As a result, they highlight the necessary pragmatism on issues ranging from internal capability development and outsourcing, to prioritising efforts based on available resources (on GDPR compliance: "*To be honest, the amount of work to be done there, and the amount of stuff that comes in is far greater than the people you've got, so the way you deal with that is you take a risk-based approach*."), recognising the distinct operational challenges posed by both policy and processes ("*at a university level*"), and, subsequently operational IT security.

4.2.1.2 Threat Perception

The frequency and impact of malicious activity are two important and sensitive aspects of the case. Threat presence is the main trigger of security efforts and adaptation, alongside legislation and compliance. However, the case is not selected based on, nor is it defined in relation to specific incidents. So, while no questions concerning attacks were explicitly asked, indicators of general threat activity have come up in several interviews. Val asserts that attacks occur regularly/"*everyday*" ("*Right now, somebody is trying to attack us*"), and are, in general, successfully defended against. From an IT management perspective, Alex highlights the uncertainty associated with discussing the likelihood of a breach having occurred: "*Can I say hands on heart that we've not been successfully penetrated? Of course I can't, cause if I had been, I wouldn't know about it. Can I say, that the business is operating, and that it's risks are appropriately managed, and that we're continuing? Yes, that's something I can measure. "*. In a more direct manner, Rudy acknowledges some, albeit limited, success of threat-actor efforts: "*of course we've been hacked. We've probably had (hacks) we don't know about yet. But nothing major*". Together, these perspectives from individuals with exposure to the available insight concerning malicious actor efforts justify an active organisational stance in relation to IS/cybersecurity. On the issue of attack vectors, the anecdotal evidence and the trends presented by participants are consistent with the sector data covered in the previous chapter, the most notable form of attack being Phishing. This pattern does not occur within the commercially focused spin off venture, which, for the 18 months prior to the interview, has been "bombarded by ransomware".

In order to address the perceived threats, University X has developed a number of measures which include functional division based on specialism, decision making support, policy, staff training, perimeter defence, technological investments, and a focus on Cybersecurity within executive recruitment profiles. The traditional ICT-based operational security defence and planning functions are supplemented with a dedicated, specialised cluster consisting of data protection specialised staff, legal support, and risk analysts. Structurally, the cluster is autonomous, and it reports directly to the executive board. The recruitment of a cybersecurity focused executive was also perceived as an indicator of commitment towards addressing the issue. On the issue of changes within the institution as a result of security

efforts, Remy, as a technical actor, notes: "*... I think a lot of change is actually driven by incidents and problems, be they within this organisation or elsewhere. […] And I mention this because we've had people join the university recently in quite senior positions who take a much more serious view of security than their predecessors*". Similarly, within the context of critiquing the security paradigms employed by the institution, Charlie states: "*I do have confidence in our new IT director because I think he's warm on the button*."

4.2.1.3 Cybersecurity Dynamics

Given the relative novelty of the threat, the effects of the university's cybersecurity efforts are described by actors in the form of changes to policy and processes, training, managerial pressures, and increased overall awareness. The significance of these changes emerges as a theme, as does its ongoing nature. Sage notes: "*…so if you started working here three years or four years ago, or ten, yeah, the practices would be different… different, completely different, so you have to adapt. And I think that [given] the nature of this topic you are learning every single day…*". Sentiment concerning these changes is less homogenous, ranging from the positive, i.e. "*… the university is doing everything to get each and every one protected*."; to the sceptical, i.e. Cybersecurity is a "*buzzword*", thus the university's stance raises concerns of "*over caution*". Participants with operational oversight highlight recent efforts to implement new operational tools enabled by technological advances, most notably Artificial Intelligence and Machine Learning. These are seen as a task-specific departure from a human-centric approach, which is limited in its ability to deal with the volume of data produced by the institution.

From a leadership perspective, the perpetual feedback loops between offence and defence which underpin the nature and pace of change requirements are seen as the driving mechanism of cybersecurity as an inherently dynamic endeavour. As the object of defence consists of a fluctuating, generally expansive base of assets, security tools evolve, and threat actors subsequently adapt their practices based on effectiveness: "*both sides need to be dynamic…*". This view is consistent with the year-on-year growth in the number of incidents at a sector level, highlighted by Brooklyn, and the unanimous perception of escalation in cybersecurity emerging from the actor interviews.

Based on the decision maker responses to change that they have encountered within the context of cybersecurity, Charlie identifies two contrasting extremes: an "*almost neurotic*" approach whereby decision makers strive to "*secure everything they can — to the extent that it impacts adversely on the way we work*"; and a "*lackadaisical*" approach characterised by a general disregard for possible impact in favour of the status-quo. Both approaches are presented as prevalent across the organisational hierarchy. The same tension is described by Val as underpinning leadership efforts, given that, at an executive level, conflicting interests converge. Furthermore, dichotomous stances amongst stakeholders are presented as a frequently encountered product of differences in responsibility, or accountability, making their reconciliation central to decision making in cybersecurity.

4.2.1.4 In-case Epistemology

The high pace of change/system dynamics characterising cybersecurity is reflected within the interview data primarily from the perspective of decision-making and risk analysis. This is a meaningful aspect of the epistemic difficulties faced by the organisation, especially within the context of the previously described adversarial dynamics. The necessity for time-sensitive action supplements the pre-requisites for awareness, coordinated intent, and pragmatic knowledge which underpin a social system's top-down responses to adaptive pressures. The idea of temporality within systemic change is also associated with the topic of knowledge validity. Charlie presents *'valid knowledge*' as being '*up to date*'. Rudy, representing a risk analysis perspective, also discusses the pace of change within the context of knowledge validity/strength: "*So, we're suspicious — we're never sure that we know everything. Things tend to change very quickly*." This lack of certainty is presented as a strength, as it justifies a position of caution and instils a necessary awareness of epistemic limitations. Pace of change is seen as meaningful for assessing the strength of the knowledge upon which prescriptive/risk claims and subsequent actions are predicated. This is due to the inherently pragmatic conceptualisation of knowledge, which anchors the notion to action, and its desired effects. As these effects relate to dynamic systems, the representations of system states that are used to inform action are inherently ephemeral.

Beyond the unanimously pragmatic interpretation of knowledge (i.e. the predecessor to action-results), several epistemological themes emerge from the interviews. Firstly, a collectivist/relational interpretation of knowledge is favoured, whereby individuals rely on the available network of expertise, which they navigate in order to reach an objective. Val uses a metaphor to illustrate this position: "*… so you've got an iPad there in front of you, that you're working. You don't know how it works inside — you might do. But most… 99.9% of people do not know how it works. You just know about its utility and you know how to use it. So, I think, as a user, what I want is to understand ahead of time what things might need to change if things need to change, and I need to understand with some confidence that there is some protection in place*". From a personal perspective, Ash notes: "*In my role (cybersecurity) Knowledge is about the risk — it's about where are the breaches likely to come. And then, knowing where to go to get help and advice. It's… knowledge is about trying to minimise the unknown unknowns. It's about making sure that, at my level, I'm aware of what I need to be aware of, and where to go to get the expertise.*"

A second theme is the recognition of context-dependent epistemic form. The association between knowledge and action with desirable effects, also implies variation in its manifestation depending on its context, even when it relates to a central phenomenon. When asked to describe cybersecurity knowledge, actors in different roles have different descriptions of the idea, all informed by what they see as potentially valuable in addressing the phenomenon within the context of their role. These include: experience, case-studies and scenarios, new attack vectors, risk, awareness of relevant occurrences and means to access expertise. Charlie illustrates this point: "*I think that knowledge needs to be different for different audiences, so the knowledge for our IT professionals, needs to be: 'How did this happen', 'What was the methodology used'. But for decision-makers who are not necessarily quite as technical, probably it needs to be the scenario driven type of knowledge.*"

The conceptual framework provides a potential explanation: in line with the Panarchy heuristic, adaptive pressures imposed by threat actors at an organisational level have different implications for behaviour selection across the levels of the hierarchy. Furthermore, these compete with the grander selectors, which, for University X, relate to the fulfilment of its primary functions in relation to its stakeholders. So, put simply, even for a common

phenomenon such as cybersecurity, in order to enable desirable action, knowledge claims must vary in form and content. This results in a sense of epistemic locality, where top-down signals must account for potential variation/distortion across levels within the hierarchy. Val's broad description of effective cybersecurity strategy ("*It should enable us to do everything we want safely. That's what it should look like — it should be about letting everybody in the organisation achieve their objectives, achieve the organisation's objectives safely*") illustrates how security enables the pursuit of primary adaptive pressures (which subsequently enable sustained system growth). However, it also carries very different prescriptive and epistemic implications throughout the various sub-systems which form the organisation.

At a more abstract level, Alex argues that there are three aspects to cybersecurity knowledge: "*the threat analysis space*", also described as "*the risk space*", "*the internal business knowledge*", and "*the technical phase*". According to its description, the threat analysis space involves actively scanning for threats, and, given the specialism and resources it requires, it is seen as a task which should be outsourced or managed by a partner company. In contrast, the internal business knowledge is inherently local, and essential for "*translating*" general threats into business specific threats. Finally, the technical, mitigative knowledge is presented as the precursor to risk mitigation and treatment, and is described as potentially encompassing "*retrospective actions*" or feedforward actions, shaping future system design choices. This makes it heavily reliant on the previous two aspects, which determine an organisation's understanding of its cyber risks, without which, mitigative practices can be inefficient, ineffective, or both. While all three aspects are generally covered by Risk Management frameworks (they address Threats, Vulnerabilities, Impact and Treatment), this taxonomy is meaningful as it is based on distinct capabilities, actors, and approaches, all centred around a singular function.

4.2.1.5 A Knowledge Based In-case Comparison

These three aspects also provide an opportunity to explore the distinctiveness of the case, from a 'knowledge problem' perspective. As a result, a broad in-case comparison can be made between University X, as a large, higher education provider, and its subsidiary, as a profit-oriented, smaller, integrated yet separate entity, through the interview data. Within the threat

analysis space, the university is favourably positioned. This is due to formal partnerships and information exchange programmes which leverage the sector's unique competitive dynamics (on threat information feeds: "*JISC have some, there are several e-mail group amongst our peers, which run by UCISA, and then we all individually follow various blogs, websites… and if something interesting [comes up] then we'll share it amongst colleagues in [IT Function] and [Dedicated Information Security Function]*"), financial flexibility which enables outsourcing to, and investing in dedicated third parties, as well as available support from sector specific bodies such as JISC.

In contrast, the subsidiary relies exclusively on informal networks, staff interest, and on the input of the University, in spite of its distinct operational model. An anecdote illustrating the threat analysis limitations of the subsidiary addresses the significant gap left by the departure of a single highly knowledgeable staff member, with a personal interest in cybersecurity: "*So in a small organisation like ours, we are, to an extent, dependent on people that they have a fundamental responsibility to security […] but to get beyond that, to have somebody that is actually scanning the horizon… you really… it depends on the individual. We'd love to be able to have someone who is doing that*". The primary focus on profit also constricts budgeting and investments, as prioritisation is based on financial ROI and clear necessity: "… *if you're looking at the difference between us and [University IT Function], then the fact that we are pretty hard-nosed and commercial is probably the thing that causes the greatest bias. For example, we don't have an IT budget. We operate on an as and when and a needs basis*".

However, the University's large infrastructure, complex operational model supported by knowledge intensive processes, its heterogeneous staff base — both culturally and experientially, as well as its adherence to values such as openness and academic freedom, all make the internal business knowledge space a challenging one. On the topic of developing a data asset register, Rudy notes: "*It's a huge, huge amount of work. It usually unknown unknowns which [are] the big challenge. We know the big systems that we have. Our big financial system, our student databases… It's the small pockets that are holding personal data particularly which is what [my function] are very much interested in. Although, […] wider people will be interested in Intellectual Property data belonging to our research partners. We hold governmental information as part of research and projects. So, although that doesn't*

concern [my function] particularly, or even GDPR, but it's still data that we want to protect and we wouldn't want it stolen. Or leaked."

When University X operational actors were asked about their adherence to formal processes and the effect it has on the predictability of their professional behaviour, several patterns emerged. For academic actors, low-variation, mature processes like teaching (i.e. lecture delivery) are seen as inherently predictable, whereas research related tasks are more opaque. From a non-academic perspective, the ad-hoc nature of many of the challenges faced was highlighted, limiting the inferential value of process descriptions. Adherence to policy and process was also highlighted as culturally informed, as actors with international experience perceive organisational culture to be more (too) restrictive within the UK. In contrast, the subsidiary operates under a significantly simpler business model which does not rely on intellectual property or informational assets, and presents an inherently clear understanding of financial streams, and of the potential impact associated with cybersecurity risks. This is also due to the significantly smaller organisational scale and higher degree of operational homogeneity. Unlike the threat space, the asymmetry between the organisations' accessibility of internal business knowledge favours the smaller, for-profit, less complex operation.

From a technical, 'mitigative knowledge' perspective, the comparison is less substantiated through the data than the previous two aspects. However, a number of noteworthy facts emerge from the interviews, mostly relating to the academic institution. University X benefits from a unique opportunity enabled by know-how, in the form of its White Hat Hacking students who are used a penetration testing resource. In comparing the nature of the institution's cybersecurity challenges in relation to the sector, and other sectors, Alex notes: "*… So that [hacking students within the network] gives you a dynamic in terms of threat, but it also gives you a dynamic in terms of opportunity. Because if we can actually have — and we do — we have conversations with our colleagues on the White Hat Hacking courses. If we can use those students… 'now if you've got a project you want to do, and you can do it in a controlled environment. Test our systems. Work with us'".*

Ash also notes that the difference in financial leeway, and the effects this has on decision

making, means that the University will be significantly better equipped from a technological perspective, whereas the subsidiary will have to justify mitigative decisions, such as upgrading systems, from a cost-benefit perspective. However, as 'mitigative knowledge' is contingent on the understanding of the threat space interpreted from the perspective of the business knowledge, accurately establishing such a cost-benefit baseline can be less than obvious. This can amplify the role of cognitive biases when considering both the likelihood and the impact of a breach, as the vividness of the main heuristic pattern described — i.e. Tangible profit is the primary objective — can affectively suppress the seemingly less concrete eventuality of a breach. While clearly stated as the most notable local source of bias in relation to cybersecurity decisions, this heuristic is by no means unique to the subsidiary. The pattern of underestimating risks prior to a breach, and overestimating them after a breach occurred is also observed at a sector level by Brooklyn, who presents it as a common. In fact, both institutions are vulnerable to the subjective, contingent nature of their action-triggering beliefs held by individual decision makers. This raises the importance of the systemic structures and approaches used to create and select for feedback across hierarchical layers. In this sense, the smaller organisation has fewer corrective opportunities, given its flatter structure, relative operational homogeneity, and the immediacy of its financial orientation.

4.2.2. The Epistemic Substrate of Cyber Risk

4.2.2.1 Rationality and Dichotomies

Beyond its implications for the role of context, nuance, and contingency in discussing the 'rationality' of organisational actors within cybersecurity, this final aspect of the comparison between the two distinct yet related institutions exemplifies an interplay of some of the study's core themes: knowledge, uncertainty, and risk as a construct. It is also worth noting at this point that, in spite of the explicit emphasis on the topic of rationality within the interviews, the concepts which have emerged from the literature review are most clearly observable within the data through adjacent topics, such as risk and uncertainty. As a result, behavioural tendencies, biases and heuristics are discussed as complementary to the other topics, and will not be covered as standalone themes. They are, however, valuable for achieving the study's second objective: developing a case-based critical understanding of the

epistemic requirements of cyber risk frameworks.

A first thematic example of the convergence between Rationality, Knowledge, and Risk is presented by dichotomies as a conceptual frame of reference which serves to add nuance to the representation of organisational cybersecurity dynamics. While not explicitly addressed by the interview questions, dichotomies were used by both decision makers and actors to express the variability of possible stances to be taken, and the sense of a cost associated with each approach. Addressing risk as the tuple of likelihood and potential impact which characterise an undesirable event assumes a sense of objective valence. However, both the data and the conceptual framework suggest that, in complex settings, the impact of local changes can be non-local, disproportional, and hard to predict. As a result, decision-makers highlight that an over commitment to security can be detrimental to accessibility, freedom, or responsiveness to change. In contrast, neglecting security is perceived as an increasingly costly, potentially existentially threatening position.

Within the case, balancing dichotomous objectives is unanimously seen as a top-down, leadership/institutional responsibility. However, any such balance must account for dynamism, evolving pressures, and interdependence, while enabling the fulfilment of the organisation's/system's primary function. Alex notes: "*There is a fundamental tension between ideas of security, data protection, that sort of thing, and the university culture, which is open, collaborative, freedom to innovate, freedom to share, all that. Those two things, you can almost draw a line and put them in opposite ends of the line*". 'Academic freedom' and its preservation are seen as a sector specific value which generally tips the scale in favour of openness. While academic freedom is, as the name suggests, a sector-specific cultural construct, within the context of cybersecurity, it is described as exhibiting a broader range of tolerance to departure from process, and an empowerment of actor choice. Neither of these two tendencies is inherently academic, and both are likely to underpin knowledge-intensive operational models outside of the sector.

As dichotomous objectives/values are individually desirable, through functional divisions, organisational structures can exhibit sub-optimisation and localised incentives. A myopic preference for one aspect of a dichotomy, without adequate consideration for its counterpart

is classified by Val as bias: "*… it happens all the time. You have — and it depends where the responsibility, or the accountability lies. If you're talking to the person who will get their head kicked in if we have a meltdown, they are very keen on one end. If you are looking at somebody who is trying to be as open and as sharing as possible, they will sit on the other side. And I think, for decision makers, it's about trying to find that — the right level… And that's difficult.*". This classification is consistent with the definition of bias presented in the literature review, as a heuristic preference is applied to a grander, different context, resulting in a mismatch.

Even amongst the interviewees, on the issue of openness vs. security, expectations varied. For example, Eli argues: "*Striking that balance is very, very important. But, at the same time, if need be, I would think that security trumps openness* ". In contrast, Charlie states: "*a large part of my thinking around this is that part of our defence is to share, and part of our defence is to be open with everything we can be*". While both actors express the importance of balance, and both share a desire for a thriving organisation, the difference in their priorities highlights the role of subjective perception when addressing shared, concrete phenomenon, and the potential conflicting views on how progress can be achieved. No ways of explicitly accounting for, or addressing bias within decision making and cyber risk analysis were identified by interviewees, in spite of the concept being recognisable, and discussed as meaningful.

4.2.2.2 Uncertainty and Predictability

This variability supplements the inherent uncertainty presented by cybersecurity. When describing this uncertainty, decision-makers presented it as either distinct from other facets of organisational activity given the scope of the "unknown unknowns" (a reoccurring paradigm amongst the responses), speed of change, and the potential impact of the unknown; or as not inherently unique, yet problematic for the same reasons. All of these characterisations are consistent with the anecdotal evidence presented by the introduction and with the assumptions made throughout the literature review. On the topic of uncertainty, epistemic granularity is presented as a meaningful variable. More specifically, at a coarse level, threat activity is generally seen as predictable, i.e. attacks are likely to occur on valuable targets. However, predictive accuracy decreases considerably when attempting to account for

the type of attack and likely impact. The unpredictability of distinct threats is presented as a key determinant of their success.

As risk analysis is partly predicated upon an understanding of event likelihood, Rudy's description best reflects the issue as applied to the case. They note: "*You just cannot see any patterns. We have… I mean our reporting is all the same proportion of each type of incident. We have about 9-10 different categories of incidents, and we have sort of the same proportion each month. But the numbers will be different.*" From the perspective of the conceptual framework, the emergence of bottom up higher-level order, such as the consistency in attack vector proportions, and the unpredictability of behaviour and volume, are both consistent with the behaviour of non-linear dynamics. This uncertainty sets the context for the conceptual application of risk, and shapes the scope and role of local implementations.

4.2.2.3 Risk Practices: An In-case View

Within the case, the notion of 'cyber risk' takes three thematic forms: formal cyber risk management efforts, which consist of explicit assessments and mitigation strategies; narrow scoped, function specific risk-based tools; and risk as a conceptual heuristic which informs the framing of threat activity, and the subsequent organisational response. The first of these is identified as part of the core responsibility of the dedicated Information Security Function (ISF), which performs risk analyses focusing on both the organisation and its suppliers, in addition to incident monitoring and pattern seeking. The output of the function informs both board-level decision making and policy, and the stakeholders of the risk assessments who are approached in a collaborative tone in an attempt to align incentives. Part of this strategy includes the framing of ISF visits as 'security health check-ups' rather than audits, and a preference for positive feedback, in a systemic sense.

Methodologically, no formal accreditation or standard is implemented, however ISO/IEC 27001 is mentioned critically within the context of subjectivity within Information Security risk assessments based on likelihood-impact grids. These are seen as highly subjective ("*you can ask five people and get five different answers*"), yet lack adequate alternatives. On this point, Rudy notes: "*A lot of these have got a simple three-point scale which I don't think is*

enough by any means, and one thing that there isn't is — I would love it if there was something, some sort of consistent algorithm where you could assess a data base, say, and put a figure, a number on the risk — a risk factor that is based on, I don't know, number of records held, how sensitive is the data contained within it, who would have access… There's something we've been trying to develop ourselves because there doesn't seem to be anything out there. Without that simple three point three grid it's… You can probably figure what your higher risk is even without doing that. We really need something a bit more sophisticated." At a more general level, an explanation for the low sector-wide adhesion to frameworks from accreditation bodies is presented by Brooklyn, who notes that academic freedom makes it difficult for compliance targets to be reached. This view is supported anecdotally through a description of an institution which failed its Cyber Essentials self-evaluation at the first step, given an inability/unwillingness to restrict admin privileges for its staff members.

The interview data indicates an ISF awareness of the behavioural limitations of Risk Assessments, and subsequently Risk Management efforts. Human vulnerabilities are recognised as a generally unintentional product of lapses in awareness of both a temporary (i.e. security is not considered when acting towards a goal) or a general (i.e. not aware of policy or threat) nature. Similarly, the cognitive variability rooted in the subjective component of cyber risk analysis is also recognised from the perspective of the analyst, as the process is "very much based on assumptions" and intuition. These are both seen as inherent forces which shape the dynamics of the problem that the ISF faces, which are coupled with the previously described uncertainty, internal business visibility barriers, lack of inherent predictability of threat behaviour, and cultural barriers to mitigative efforts. The abundance of perceived relevant variables and the permutations of their locally manifested weights lead to a preference for modularity in the selection of operational and conceptual tools. The resulting, analyst-oriented approach enables leveraging subjective experience and expertise to account for known sensitivities and nuance, without the procedural homogeneity of methodological orthodoxy. So, rooted in a pragmatic, problem-oriented epistemology, the selection of tools and procedures is driven by opportunity, as well as contextual knowledge and feedback.

A key challenge for ISF mitigative efforts lies in the process of communicating analytical

outputs. Once policy has been developed, it must still be effectively disseminated amongst stakeholders in order to instil the desired change. On this issue, Rudy notes: "*The university has its sets of policies that are not known to everyone. It's all very well having a great set of policies that are beautifully written, […] but if it's not applied, and if people don't even know the way they should be behaving, then those policies are worth nothing. And this is a big challenge — it's education, it's training*". The notion of academic freedom, which affects the feasibility of restrictive measures and controls, shifts the balance of risk mitigation to individual awareness and voluntary compliance, as bottom-up efforts. However, the general actor interviews indicate an unanimous expectation of top-down cybersecurity support, while both capability and liability are delegated to an organisational function, i.e. ITC or ISF, with the exception of scenarios describing user incompetence.

The role of communication in the utilisation of mitigative knowledge is also highlighted by Charlie, who argues that 'good' cyber risk management is "meaningful to people", and enables stakeholders to answer "why should I care about this?". This statement seems related to the previously covered discussion over the context dependence in forms of 'effective' knowledge. They also present the ICT policies as "something that people just roll over and forget about". Similarly, Sage expresses scepticism over the value of "ticking boxes", as such methods are limited in what they can address, and cannot substitute individual responsibility. Thus, two-way communication streams are a key enabler of cyber risk management frameworks, through their role on increasing operational transparency for the benefit of analysts, facilitating feedback exchanges, and ensuring that mitigative knowledge is disseminated in a context-appropriate form. In a large organisation like University X, the potential use of informal networks and personal exchanges for this goal raises concerns over efficiency, consistency, and scaling.

Within the context of corrective feedback and mitigation-oriented decision making across hierarchical levels, Charlie highlights that reports concerning the organisation's cybersecurity are only circulated at a senior-management level. This limits the exposure of other actors to such information, and thus affects their awareness and perception of the problem, while suppressing their ability to develop and adapt contextual heuristics: "*So, therefore, we can develop our own heuristics on a different set of information, and I think until the information*

is comprehensive across the audience, you're always going to have those individual contextualisation of how people react […] *because you don't know about the threats, you don't have the information to change your heuristics. So that's an interesting one because it's around communication. If you want people to change behaviours, you actually need to give them the information to prompt them to change those behaviours, or attitudes, or approaches.*" Efforts to improve knowledge-sharing and collaboration amongst organisational functions (ISF and IT) are underway, as the development of a centralised knowledge-base is part of the vision of the ISF. This should contain "*all of the risk assessments, third party compliance, due diligences, instant reporting…*" as well as processes and policies. The existence of such a resource has the potential of significantly simplifying risk mitigation and communication efforts, while highlighting potential gaps.

The second thematic occurrence of Risk within the data is a derivative of the first, in the form of function specific risk-based tools or heuristics. These include traditional aspects of cyber risk management frameworks, which are selectively used to achieve a specific function, and serve as explicit, shared heuristics. An in-case example of this lies with the IT function's view of risk assessments, which consist of likelihood and impact score matrices, as "useful" prioritisation and communication tools. However, "you can't get too hung up on" them given their lack of depth and the methodological distortion resulting from the reduction of risks to single values. So, the same aspects which serve as function-specific strengths — i.e. simple quantitative comparison for prioritising investments, and communicating specialised information in a general manner — are also weaknesses in wider contexts. This behaviour is consistent with Gigerenzer and Brighton's (2009) description of ecological rationality, or contextual fitness, as a determinant of heuristic effectiveness.

In this sense, the difference between the two views on likelihood-impact cyber risk assessments (IT — functionally adequate; and ISF — generally inadequate) is attributable to context. The IT function is operationally focused, and it benefits from a smaller gap between analysis and action in its primarily operational function. Thus, as a setting, it prioritises efficiency in resource deployment and diagnosis efforts, as well as an ability to quickly communicate the dynamics of individual risks internally, for a relatively homogenous actor base. In contrast, the ISF's function is primarily analytical, as it provides insights across a wide

range of stakeholders. It is also expected to collect operational information, represent nuance, and relay its findings in the form of reports. In addition, its primary function is knowledge-centric, inferential, and rooted in the uncertainty of Information Security. While Information Security is undoubtedly a focus of the IT function as well, its primary function is ensuring the optimal performance of the organisation's ICT infrastructure. Thus, given the environmental pressures faced within the two related environments, the same heuristic yields different perceptions of adequacy. Furthermore, when noting the difference between the two functions, it must be noted that they actively cooperate and aim to achieve complementary functionality.

Finally, the third thematic occurrence of Risk lies in the underpinning structure and language used to frame threat activity and subsequent organisational response scenarios. Indicative of exposure to Risk Management frameworks and training, instances of this theme were noted in the framing used by technical actors and decision-makers. Unlike the previous two, it entails a more abstract perspective, without reference to a specific event, framework, or tool. As a result, it could indicate that, even outside of the confines of a formal organisational effort, risk management methodologies serve as a heuristic lens for interpreting cybersecurity related offence-defence dynamics and condition the mental models of key actors. It is worth noting that the effects of pre-interview priming could also influence the framing of responses, as participants were briefed that the subject of the study will include 'Cyber Risk Management'. As a result, the meaningfulness of this final aspect in relation to the interview data is hard to establish with confidence, and will not be emphasised. However, the risk-conditioned intuitive heuristic framing of cybersecurity seems subjectively plausible for actors with some involvement in the field.

Outside of these functions, Charlie notes that they have not witnessed a general risk-based approach: "*… it [Risk consideration] does tend to be very contextualised. I've not seen a general approach towards risk. I haven't come across conversations where we're talking about strategies and policies and ways forward, that actually look at risk. It doesn't seem to be part of that conversation. You know, what's the risk of doing it, what's the risk of not doing it. That's never come up in conversation. […] It's the only organisation I've worked in where that doesn't happen — or doesn't at my level.*"

4.2.2.4 Adaptation and Adaptivity

As the final topic covered by the data-collection strategy, Adaptation was relationally described as a function of Change, Knowledge, and implicitly Risk. In this sense, the logic of the framework positions 'Adaptation' as inherent in dynamic social systems (i.e. organisations), given that changes in the adaptive pressures must be perceived and conceptualised, potentially through heuristic functions such as Risk Management, in order to determine top-down uncertainty navigation strategies. In addition to the process of adaptation, the data indicates actor consideration for adaptivity (adaptive capacity) as a systemic attribute. This consideration does not only address the organisation, its systems and functions, but also the attributes of risk frameworks.

In fact, adaptive mechanisms are described at all levels of decision-making, as exemplified by the previous outline of the dynamics of dichotomies. But the interview data most notably addresses the perceived importance of adaptivity in relation to cybersecurity as would be predicted from the conceptual framework. This includes subjective emphasis on its key role when considering the future of cyber risk management ("*Your word — 'Adaptive' Cyber Risk Management is going to be really, really key…*") which is seen as being predicated on a foundation of institutional situational awareness ("*gathering and analysis function*") that enables knowledge sharing and serves as an adaptive trigger for actors, systems and policy.

The link between the organisation's epistemic confidence in relation to adaptive strategies is highlighted in a manner that is consistent with the literature. Ash describes the absence of certainty (known unknowns) as a trigger for perpetual environmental scanning within the context of the subsidiary. Awareness of the epistemic limitations which underpin the local understanding of the cybersecurity climate instils a predisposition for continuously gathering information, rather than relying on static models and conceptualisations. Concerns over framework rigidity were also raised when considering 'excessive' formality in cyber risk management efforts. To this point, Ash notes: "*Something as diverse and full of as many unknowns as [cyber] risk — the bigger the framework, the more comprehensive the framework, the more used it will be and the more assured you will be that you had as much*

covered as possible. I do sometimes think that if you're too formulaic and you've got too much reliance on something that is structured and mechanistic that you could well be at risk of missing something because it could make you complacent. "

This overarching thematic strand addresses adaptation and feedback as functions of learning, which is consistent with the systems-theory framing. In this sense, "adaptability" is described as an empirically driven, experiential knowledge-process, which is "the real key to doing risk" given the fast pace of the dynamics of cybersecurity. Interviewees generally failed to identify a direct relation between adaptivity and resilience — a counterintuitive fact given the literary links between the concepts. This indicates a local perceptual predisposition more than anything else. Nonetheless, it serves as a reminder that, within organisations, potentially colloquial terms such as 'adaptability/adaptivity' and 'resilience' can have a different meaning than that prescribed by the literature. Overall, within the case data, facilitating adaptation is linked to an awareness of the unknown, the maximisation of feedback streams, acknowledging pace in a manner that corresponds to the temporal utility of knowledge, and correcting for deviations between intent and results that are rooted in non-linearity, or inadequate representational models.

Significant variability is shown in descriptions of what feedback consists of, and what its acquisition entails. Non-technical actors invoked seeking the assistance of "experts", "IT guys" and "the IT department", however only one participant could give an example of such an exchange having taken place. When asked if they are aware of any formal policies or processes concerning general cybersecurity feedback exchanges such as reporting vulnerabilities (described loosely), or seeking advice, responses were hypothetical and intuitive, describing informal contact through e-mail or phone. No clear evidence of a concrete, demonstrable understanding of the available cybersecurity knowledge network could be identified for participants who are not exposed to it as part of their role.

It is worth noting that informal contact with an organisational function is not argued to be an inherently ineffective primary feedback strategy for actors. However, it does impact the frequency and nature of any informational exchanges, and, ultimately, affects wider awareness of issues, resources and policy that are not directly communicated in a top-down

manner. Given that such formal approaches are constrained in scope and frequency, actor situational awareness is largely a matter of personal experience and informational exposure. So, in spite of the declared openness of actors towards collaboration and engagement with the IT function, both their lack of awareness concerning policy and feedback procedures and their limited technical awareness affect the likelihood of voluntary feedback exchanges.

Two further aspects emerge on the issue of feedback amongst functions and actors as a driver of adaptation: the plurality of the declared adaptive reference points across interviewees, and the efficacy of the communication process. The former is an extension of the previously discussed dichotomies, and reflects the variation in the perceived object of concern and performance indicators across the organisation. While decision-makers accounted for threat behaviour and the achievement of corporate strategic objectives, actors described a narrower, internal orientation, seeking calibration from internal compliance proxies. This is an intuitive pattern, as it corresponds to the variation in organisational roles. It is nonetheless noteworthy, as top-down intent and policy must account for the potential of distorted adaptive triggers, and for misfires in their dissemination.

The latter aspect — the role of organisational communication mechanisms for adaptivity — is an underpinning theme in participants' descriptions of what 'effective' cybersecurity strategy and behaviour entail. However, decision-makers with direct cybersecurity oversight, such as Val and Alex, emphasise the nested strategic nature of cybersecurity efforts within the grander levels of organisational planning (i.e. the cybersecurity strategy is based on the ITC strategy, which is designed to enable the organisational strategy). As a result, an implicit aim is to minimise the footprint of operational disruption attributable to both threat behaviour and defensive efforts. The need for moderation from this balancing act which subjects cybersecurity to the organisation's primary value generation functions, also shapes the perceived extent of feasible staff training, awareness and preoccupation. The aim of this operational branch is to minimise disruption, while enabling the pursuit of the essential operational functions.

Val articulates this broadly in his previously mentioned description of an 'effective' cybersecurity strategy: "It *should enable us to do everything we want safely. That's what it*

should look like — it should be about letting everybody in the organisation achieve their objectives, achieve the organisation's objectives safely." Other such descriptions include: "Contextual" and "appropriately communicated", developed part of a conversation with stakeholders; Policy and procedure driven, supported by training and awareness maximisation coupled with periodic stress-testing; Effectively communicated, leveraging expertise; All-encompassing — beyond technical (holistic), coupled with awareness development; Based on an understanding of the specific level of risk, top-down driven, balancing training and education with policy, with a consideration for cost; Integrated to, and based on an understanding of business models and the operational lifecycle.

Throughout the interviews, communication emerged as a common denominator for all the topics of enquiry. Within the literature review, the central role of coordination, and implicitly communication, within social systems was highlighted. This point is also observable within the research-context through the emphasis placed on knowledge networks as the main enabler of security efforts. Even through a high level view, in-case cybersecurity oriented functions rely on partners (internal and external) and vendors for threat related knowledge, actor compliance and contact for abstracting business knowledge, leadership support in order to appropriately scope resources within the organisation's wider strategic context, and internal communication for the consolidation of shared situational awareness and the dissemination of mitigative feedback.

So, under the previously described uses of risk constructs lies an epistemic ecology supported by a network of formal and informal relationships and interactions, all driving adaptive behaviour with varying degrees of efficacy across the systemic layers of the organisational hierarchy. Given the context bound, function-driven nature of risk as a heuristic, there is no objective foundation of inference for the traits of an abstract 'effective' cyber risk implementation or cybersecurity strategy. On this point, Rudy notes: "*You can't [distinguish a 'good' or 'effective' cyber risk implementation] … It's certainly good and it's successful until something goes wrong and someone gets in…*". This statement aims more to dispel a potential positivist, absolutist framing of strategy within cybersecurity, rather than propose that all strategic avenues are undistinguishable or doomed to fail. In fact, Val's conception of 'effective strategy' aims to nullify cybersecurity as a 'disabling' factor, while

integrating it within a homogenous operational approach. This framing is a culmination of a dynamic and complex narrative, shaped by dichotomies, judgement calls, and ever changing threats, while adaptive efforts are harmonised within a network of complementary specialism. The epistemic gap filled by strategy is, thus, non-trivial, time sensitive, local, and evolving — especially from proactive stance.

The case-data also shows a range of positive indicators, or enablers, which underpin the efficacy of existing tools and approaches. These include context-specific opportunities, such as the highlighted use of White Hat Hacking students and IS faculty expertise, in addition to the ongoing information exchanges pertaining to information security with other institutions within the sector. Furthermore, the threat climate was described as moderate when compared to other, more turbulent sectors (i.e. financial) given the non-monetary nature of most of the informational capital. The absence of clear monetisation pathways serves as a disincentive for a number of threat actors. In addition, an institutional commitment to the issue of information security was visible. While the previously described conceptual limitations of cyber risk constructs are not explicitly addressed within the case, key staff, including decision makers and risk analysts demonstrated an awareness of their effects.

Such limitations include defining actor behaviour in terms of assumed normative behavioural pathways (addressed within the literature review as actor 'rationality'), assumed environmental linearity and sensible predictive consistency, and a difficulty in reconciling incentive misalignments and informational asymmetries. In response to these limitations, the role of individual expertise is emphasised over shared heuristics and frameworks. Thus, the latter primarily become communication and knowledge externalisation tools, usable to simplify otherwise complex information.

At an abstract level, the inferential mechanisms of the core explicit heuristics (i.e. formal quantitative risk assessments) are replaced, or at least supplemented with decision-maker dependent tacit heuristics (subjective risk assessments), which are implicitly qualified as more effective for the task, while the explicit structure is maintained to codify knowledge claims and enable action triggers. In simpler terms, if the risk analyst can formulate a more nuanced and contextually adequate interpretation of the problem situation based on available insight

and experience than that yielded by the use of formal frameworks, the latter will be used in a limited manner, as exemplified by the case. However, this raises issues such as scalability, variable pace of change, cognitive and epistemic limitations, and informational opaqueness for other knowledge-network nodes. The following chapters will discuss the conceptual and prescriptive implications of these findings.

5. Framework Development: The Strategic Knowledge Problem

The framework development section addresses the final research objective by leveraging the outputs of the previous sections towards the development of a practice-oriented contribution. This is accomplished through two sub-chapters. The first explores the patterns of convergence between the theoretical content of the literature review, the conceptual framework and the case findings. These patterns are then used to outline the requirements and implications of the study for the development of a novel framework that employs an theoretically consistent/adequate set of systemic and behavioural assumptions regarding organisational cybersecurity. Subsequently, the second sub-chapter integrates these patterns as the foundation of an epistemic conceptualisation of Adaptive Cyber Risk Management. More specifically, it encapsulates a gradual process of theory consolidation, as each dimension of the framework is progressively introduced. The chapter is concluded with a commentary addressing the rationale behind the framework generation process, and the potential applicability of this final research output for practitioners, as a function of compatibility with existing standards/guidelines, flexibility to the characteristics of the implementation, and potential utility once implemented.

The third objective of the study is to create a prescriptive framework which addresses the theoretical (context-construct) gap identified through the literature review and the subsequent empirical exploration. The nature and generality of such a framework are both predicated on the validity of its assumptions concerning the ontological mechanisms manifested in a defined context as the basis for inferred value. Thus, the discussion of the practical implications of the study's findings, will be preceded by a brief revision of the progress.

The study's primary assertion informing all subsequent progress is a diagnosis of a problem: organisations are poorly equipped from a conceptual standpoint (construct) to deal with

cybersecurity in a top-down, strategic manner (context). While broad, this statement is supported by an exploration of the hostile epistemic landscape navigated by decision-makers, whose inferences shape the choice of strategic pathways. The literature-informed individual patterns which underpin said hostility are conceptualised in three dimensions: the ontological non-linearity of cybersecurity dynamics, the behavioural heterogeneity exhibited by actors, and the contextual potential (in)adequacy of broad Risk-based heuristics and models which inform uncertainty navigation strategies. These dimensions are used to re-frame the premise of the study: a need to explore cybersecurity as a phenomenon-derived knowledge problem.

While seemingly dystopian, the picture of uncertainty and (inherently limited) knowledge painted through this frame of analysis also carries prescriptive meaning. It calls for contextual adaptation in the implicit epistemology, conceptual tools, and underpinning assumptions which inform top-down organisational understanding and behaviour. In light of this, the case provides a lens for the evaluation and consolidation of the postulated mechanisms driving the dynamics of the problem, as it presents an in-depth perspective of the interaction between context and tendencies. At the point of interaction between the theoretical foundation of the study and the case data lies a mix of general and local patterns. Both were briefly highlighted in the previous chapter. The distinction and elaboration of these patterns sets the ground for the final, prescriptive research objective.

5.1 Patterns of Convergence: Case and Theory

5.1.1 Ontological Complexity

The first such pattern lies in the non-linear dynamics view of the cybersecurity ontology. This has direct implications over the uncertainty faced by organisations, as it affects the nature, predictability, and emergent demi-regularities exhibited by security incidents. Given the scope of cross-hierarchy interaction, cyber complexity is inherent in most organisations from the perspective of the conceptual framing. Notable exceptions include circumstances where the business model, operational scale, resource availability, or security orientation significantly constrain such interactions. Indicators of complexity within the case are found across the case groups, as anecdotes, views, or procedural descriptions. Briefly, these include: the lack of predictability of incidents; the reliance on subjective measures of likelihood evaluation, absent grounds for objective measures (i.e. probabilities); the difficulties associated with impact assessments given the networked nature of systemic behaviour; the centrality of adaptation as a function-specific strategic objective; the plurality of competing adaptive pressures and feedback streams, which are often dichotomous, as well as their context specificity; and, the emergent patterns of demi-regularity which are level-specific and lack a pragmatic mechanistic understanding.

A second point of convergence addresses the role of temporality in the manifestation and understanding of organisational cybersecurity phenomena. If bound by action towards a desired effect, knowledge concerning cybersecurity, as a highly dynamic non-linear phenomenon, is in itself temporal, rooted in a specific configuration of representations. The sustained adequacy of these representations which underpin strategic inference relies on their adaptation at a pace that matches that of the change in the environmental segment they describe. Alternatively, this can also be achieved if they describe consistent regularities of said environment (i.e. mechanisms). Distinguishing between the two carries significant implications on the calibration of feedback cycles, and the architecture of implementation for risk constructs. This point is made in a less abstract manner within the case on the topic of change, and ‘knowledge validity’, and constitutes an important prescriptive implication of the theoretical perspective taken.

Thirdly, the theoretical stance can be used to infer a need for emphasis on Adaptation and Adaptivity as strategic objectives, given the role of non-linear dynamics and temporality. This emphasis is also reflected in the interview data as decision-makers frame adaptation as a central objective. However, the data provides limited insight for how this is/can be achieved. From a top-down perspective, a high-level view of adaptive mechanisms entails a mix of interrelated epistemic concepts, such as knowledge, feedback stream architecture and functional 'meta-cognition'. Analogous to its original meaning in cognitive disciplines, the latter concept is used to describe an organisation's critical awareness of its epistemic processes. Within the context of cybersecurity, this implies an ability to establish the grounds for inference, understand the limitations of available knowledge, and link it to the outcomes of behavioural pathways. It also corresponds to the previously introduced adaptive-toolbox construct (Gigerenzer and Brighton 2009) in its structural archetype for developing and adapting heuristics in complex, evolving environments. A meta-cognitive analogue is particularly important in reconciling adaptive pressure plurality, manifested as dichotomies within the case. It is also important in retrospectively distinguishing environmental determinism, i.e. outcomes that are independent of the organisation's pragmatic choices, (i.e. breach due to 0-day exploit) from actionable feedback.

However, an emergent limitation of the conceptual framing — more specifically of the complex/systemic view of the organisation, lies in the 'hard', high-level view of social systems behaviour, through emphasis on coordination and foresight. While not invalidated by the case data, this approach seems to lack flexibility when describing the cybersecurity phenomenon at multiple levels of conceptual granularity. More specifically, it fails to provide a nuanced picture of the 'softer' aspects of (lacking) coordination, including power-structures, culture, and incentive misalignments, as it offers no direct account of any such phenomena. Furthermore, an isolated, high-level view of foresight in social systems could also make it seem like a relatively homogenous (social) systemic property. This, unsurprisingly, conflicts with the case data, which indirectly presents foresight as an actor-based property that is epistemically conditioned and structurally moderated to yield an organisational capability. Again, this is not incompatible with the Panarchy heuristic, but it is also not clearly implied by it, and must be accounted for when exploring the prescriptive implications of the theoretical stance.

5.1.2 Bounded Rationality

A key area of enquiry grounded in the literature review is the critical stance on assumed actor 'rationality'. March (2006:202) argues that, organisational studies use 'rationality' to describe action "derived from a model-based anticipation of consequences evaluated by prior preferences…". The term is used throughout the study to describe the implicit representational models used to infer actor behaviour in relation to cybersecurity. The data collection strategy addressed such models both explicitly, through direct questions over normative behaviour patterns, perceptions of bias and heuristics, as well as implicitly, by comparing the direct and indirect assumptions that each interview group made about the others.

The case data and the theory converge in a variety of areas, which include the declared presence and concern over bias within cybersecurity decision-making, as well as the predicted and encountered variability and opacity in actor behaviour (understanding, and perspective). These indicate the limited inferential power of processes and systems as behavioural predictors, and justify the perceived utility of heuristics as tools within the uncertainty presented by cybersecurity. Furthermore, the Business Knowledge dimension of cybersecurity procedures within the case relies on behavioural representational models, in the form of role and process descriptions. The degree of perceived accuracy that these present was described by actors as dependent on the maturity and linearity of the task, the expectations of the role, and on the tendencies and attributes of the individual. These points reflect a need for integrating a behavioural variable of analysis within prescriptive models — especially when the aim is to establish the likelihood of behaviour-moderated anomalous events.

However, as a topic of enquiry, 'rationality' (as defined) has been difficult to explore within the case. This difficulty was most visible when querying participants' views and experiences on constructs such as biases in cybersecurity decision-making. Questions presume a shared foundational understanding of the constructs they address. While the absence of such an understanding can be mitigated against by including an overview of the concept within the

interview, this process can also bias responses, and prime participants' stance, especially when the topic presents an implicit (negative) affective response — i.e. bias. As a result, a more colloquial interpretation of the constructs was used, shaped by the participants' understanding. In relation to 'bias', this has enabled the capture of a different, context rooted description. The construct was most notably seen as a tendency to favour specific courses of action beyond what is externally or 'objectively' perceived as reasonable. The resulting view positions biases as not only a function of (deviation from) normative cognitive processes, but also of epistemic availability, incentive structures, and of contextual awareness. This interpretation is pragmatically useful, as it accounts for the epistemic context of the decision-maker, which is relevant when exploring knowledge networks and behaviour through an organisational lens. Despite its perceived presence and significance for cybersecurity decision-making, the construct is not explicitly accounted for, or mitigated against in decision-making support structures and procedures.

Another point of convergence between the assumptions brought forward through the conceptual framework and the in-case findings consists of the (declarative) importance of 'intuition'. Again, the construct has been taken out of its cognitive-science conceptual context in an attempt to explore its perceived importance for cybersecurity decisions made by actors. Intuition, in a colloquial sense, was unanimously seen as present for at least some decisions affecting cybersecurity. However, the sentiment on this issue was mixed, ranging from a positive view of intuitive insight, to a negative perception of intuition as a shortcut and a failure of 'rationality'. Even within the context of Risk Analysis, intuition was presented as a potentially valuable epistemic navigation tool, given the high levels of uncertainty faced. However, its role in reaching a specific conclusion is masked, even when the Risk Analyst is aware of the function it plays for given epistemic outputs.

When discussing the idea of Risk as a product of Likelihood and Impact of an unwanted event, the inability to calibrate for local agency-derived behavioural variability emerged as a core limiting factor of cyber risk frameworks. In a volatile, high pace, high impact domain, agency-induced deviation can have disproportional effects, even if assuming it to be a low-frequency occurrence. This highlights the importance of epistemic support mechanisms that are anchored in the local parameters of the problem they address. Subsequently, it justifies a

move beyond implicit assumptions within the analytical process, whereby incident-based calibration is subjective, and prone to hindsight bias. While the case study is potentially limited in the depth it can provide on issues of cognition and awareness through direct participant engagement, the implications of a behavioural lens for prescriptive construct development must include a procedural recognition of intuition, heuristics, and agency. In addition, the potential discrepancy between analytical outputs (knowledge claims) and actor/analyst position (beliefs) further highlights the relevance of organisational cybersecurity 'meta-cognition' to moderate feedback and support adaptation.

5.1.3 Cyber Risk Constructs

The final dimension of the conceptual framework relates to the role of risk frameworks in organisational cybersecurity. Given the methodological variability associated with cyber risk analysis, emphasis will be placed on general, framework agnostic points raised through the literature review and the case study. The first pattern of prescriptive significance lies in the functional boundaries of cyber risk as described within the literature review. Based on the ontological framing and agency-associated behavioural variation, the core components of likelihood and impact are limited by the (deep) uncertainty of the events they describe. Within the case, a critical awareness of this dynamic was exhibited, particularly within the dedicated cyber risk function, where a heuristic interpretation of risk is employed. Even at a sector level, institutions pursuing an accredited cyber (IS) risk framework are a (growing) minority. However, risk assessments are perceived as useful communication and prioritisation tools — a structure to externalise and disseminate insights. In addition, risk management terminology was used by the interviewees to describe relevant phenomena. This indicates the permeability of the risk archetype as a mental model used to interpret and contextualise cybersecurity related occurrences.

The second pattern of prescriptive significance lies in the epistemic dependencies of risk constructs. Given their reliance on contextual operational knowledge, as well as an understanding of relevant threat activity, the utility of risk analysis outputs is dependent on the effective navigation of a knowledge network. The availability, scale, and properties of such

a network all seem local to varying degrees based on hierarchical granularity (i.e. sector networks converge through institutional nodes, such as JISC). However, while implicitly acknowledged, this epistemic substratum of risk analysis is not explicitly accounted for within the context of procedural feedback. As a result, the properties of the information stream used to produce cyber risk knowledge claims are largely internalised by the analyst. This process restricts the operationalisation of epistemic metrics to guide the adaptation of inferential procedures (i.e. risk analysis). Furthermore, the absence of an explicit association between the epistemic composition of core knowledge claims and subsequent risk assessments limits the development of a shared 'meta-cognitive' intuition of epistemic confidence, and procedural consistency.

The deep uncertainty posed by cybersecurity as a phenomenon constrains the probabilistic potential of the risk archetype. Nevertheless, risk constructs hold utility as a communication tools, heuristics for effort prioritisation, and overall knowledge claim construction procedures. Given the in-case emphasis on communication, the pragmatic value of the risk archetype is clear. However, as the dynamics of cybersecurity entail complex inferences, a context-appropriate heuristic interpretation of risk, coupled with an emphasis on its underlying epistemic dynamics present an opportunity for formulating a theoretically coherent cyber risk-based approach of adaptive inference. Such an interpretation requires an awareness of the epistemic network required by effective inferences within the domain, the boundaries imposed by deep uncertainty, an orientation for adaptive mechanisms, and a nuanced view of the convoluted environment of incentives, awareness, and intent driving the behaviour of individual actors within the space. Furthermore, this also entails a meta-cognitive function, with the aim of gathering feedback on the organisation's cybersecurity epistemic performance (assumptions, knowledge and uncertainty).

5.2 Formalising Adaptive Cyber Risk Management

5.2.1 Risk and Complexity: Heuristic Underpinnings

Accounting for complexity, deep uncertainty and social dynamics in decision-making approaches involves a shift from a priori, model-based structure, towards the integration of adaptive mechanisms (i.e. Cox 2012). March (2006) provides a critical outlook on the assumption that strategic action must involve a model-based evaluation of likelihood, outcomes and preferences. In accordance with the outline of risk-based constructs, the author presents three core components of the "technologies of rationality" built from this view: *abstractions*/models (representations) of the objects of analysis and their causal relationships, and the range of choices they present; *data*, which contains a history of the organisation, and its environment; and, finally, *decision rules* (procedures), whereby intended outcomes are associated with a course of action. While March's (2006) critique of technologies of rationality is largely based on their inefficacy in complex settings, he also highlights that adaptation seeking strategies as an alternative can result in a counter-productive myopic risk aversion (i.e. maintaining status quo).

As the central requirements of adaptation are the reproduction of 'success' and the generation of variety, experiential learning, imitation, and selective replication strategies all favour the local preferences, threats, opportunities and outcomes of the adaptive agent, rather than those of the ecosystem. From this perspective, variation-seeking can be locally maladaptive while globally adaptive. The selection criteria conflicts faced by the adaptive agent must also be accounted for when attempting to deconstruct selective performance. This phenomenon is shown by the dichotomies described within the case, and the incentive misalignments described by the cybersecurity economics literature. Given its secondary role in value generation, agent-level cybersecurity adaptations can yield a lower short-term selective advantage than primary function achievement adaptations. So, purely adaptive approaches are likely to under-react to possible cyber threats, and over-react after a breach has occurred. This behaviour was also anecdotally highlighted at a sector level within the case-study. Furthermore, agent/actor adaptive pressures within organisations are structural, functional, and level-specific, so they are likely to favour same-level, as opposed to holistic

adaptations. This yields a contextual necessity for hybrid approaches/constructs which enable adaptivity while maintaining inferential mechanics. (March 2006)

5.2.2 Adaptive Risk Management: Principles

At the intersection between adaptation seeking strategies and technologies of rationality lie approaches like adaptive management. Given its emphasis on empirics, learning, and uncertainty mitigation, adaptive management is presented within the literature as a notable approach for managing complex systems — most commonly in ecological/environmental studies (Linkov *et al.* 2006, Wintle and Lindenmayer 2008). As per March's (2006) archetype for technologies of rationality, adaptive management entails establishing management objectives that are revised on an ongoing basis, (competing) models of the system, a set of strategic choices, outcome monitoring and assessment, and a platform for stakeholder involvement and learning (Linkov *et al.* 2006). This enables accelerated learning cycles, a set of evolving models of the systems, hypothesis testing and a pragmatic linkage between the range of strategies, competing system models, hypotheses and outcomes. In addition, the various implementations are closely monitored, which reflects the recognition of uncertainty, and the low degree of confidence in assumptions. (Linkov *et al.* 2006)

"The important point that we need to reflect on is that such apparent powers of prediction, as implicit in deterministic models, is only real if, and only if the assumptions made in achieving it are in fact true. In other words, the real uncertainty that may characterise the long-term evolution of an ecology, economy, market or firm is only banished by assumption. In this light therefore, we must admit that understanding and predictions will only hold until things change and our expectations are confounded. " (Allen and Boulton 2011:173)

Thus, adaptive management is indeed a technology of rationality, but one that recognises the fluidity of complex systems and their context, and the effects that it has on model-based decisions. At its simplest, adaptive management involves the incorporation of mechanisms for perpetual feedback seeking, and explicit validation procedures for the assumptions made to mitigate the uncertainty faced in applied, complex settings. As a result, it has been deemed

both compatible with, and potentially complementary to risk analysis (Wintle and Lindenmayer 2008, Bjerga and Aven 2015). This intersection results in Adaptive Risk Management, which is methodologically premised on the application of the previously mentioned components of Adaptive Management to expand and manage the measures of Likelihood and Impact/Outcome within deep uncertainty (Bjerga and Aven 2015). However, the practical implications of this convergence are not well explored within the literature. Furthermore, given the colloquial nature of the terms, and the conceptual utility of associating adaptivity and risk, “Adaptive Risk Management” approaches, like Baracaldo and Joshi (2013), can employ the notion without adhering to a conceptual lineage.

This results in the absence of a shared understanding concerning what Adaptive Risk Management entails prescriptively. For example, Ulieru and Worthington (2006) propose an Adaptive Risk Management System built around the cyclicality of the Risk Management process, which, through interaction with “risks, infrastructure and support holarchies”, accomplishes continuous improvement. The emerging concept is seemingly envisioned as a (potential) software product to be used by critical infrastructure organisations, which leverages their properties as Complex Adaptive Systems. However, the systemic autonomy in conducting and adapting the risk management process envisioned by the authors is a significant departure from the in-case ‘reality’ of risk-constructs explored in the previous chapters.

In contrast, ‘Adaptive Risk Management’ is also used to describe the final ‘Implementation Tier’ of the NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity. The document positions 'tiers' as indicative of the sophistication of cyber risk practices, but not as necessarily representative of their maturity. Within it, an Adaptive Risk Management implementation is characterised through: cybersecurity practices that account for previous lessons and predictive indicators; continuous improvement supported by ‘advanced’ cybersecurity practices and technology; active adaptation and timely response to the changing cybersecurity environment; an organisation-wide commitment to risk-informed practice concerning cybersecurity events; an evolving risk culture supported by an awareness of relevant information, and system activity; and active information sharing and consumption practices across the stakeholder/partnership network. As the scope of the Framework is

practice oriented, and the overview provided is purely descriptive, the perspective provided is limited in its potential contribution to the establishment of an academic Adaptive Risk Management narrative, beyond offering a point of reference for what an effective interpretation of the construct might entail. (NIST 2018)

Thus, in spite of their shared stated outcome, the scope of Adaptive Risk Management practice varies significantly across sources. Bjerga and Aven's (2015) description of the concept supplements traditional Risk Management (Likelihood and Impact, or Consequence and a measure of Uncertainty) by explicitly emphasising the strength of knowledge which conditions the analytical outputs. In addition, they present the adaptive risk management process as an active one (as per the Linkov *et al.* (2006) distinction between active and passive adaptive management) where the background knowledge can change as a result of the process actors and their ability to engage in targeted knowledge seeking and validation. This results in a continuous rather than discrete interpretation of both the epistemic foundation informing risk analysis, and of the Risk Management process itself.

Moreover, by explicitly establishing the measure of Likelihood as inferred from, and thus conditioned by a specific knowledge configuration, the specific behaviour of the system can be linked to explicit claims, thus serving as an epistemic validation mechanism. Furthermore, assessments built on weak knowledge can be differentiated and managed accordingly. At an aggregate level, the emerging assessment of cybersecurity knowledge and its efficacy in driving action towards set outcomes is functionally analogous to meta-cognition. Knowledge about the existing and potential performance of epistemic processes is central to the functional (cybersecurity based) pursuit of balancing exploration with exploitation — a central requirement of effective adaptation (March 2006).

5.2.3 Adaptive Cyber Risk Management: Situational Awareness Through a Knowledge Network

At the intersection between the NIST (2018) descriptive account of Adaptive Cyber Risk Management, the methodological insights proposed by Bjerga and Aven (2015), and the

overview of the case study, lie the systemic requirements and the potential utility of such an approach. A first core insight produced by the case which affects adaptive cyber risk management practice is the non-locality of cybersecurity knowledge. As the respective loci of the 'threat knowledge', 'business knowledge' and 'mitigative knowledge' are not necessarily convergent, an adaptive understanding of risk as conditioned by knowledge entails a recognition of its relational, networked nature. This principle is compatible with both adaptive management and risk management, yet it is not inherent in either construct. A knowledge-network view entails that the utility of knowledge depends not only on its availability but also on its spatiotemporal positioning and accessibility for other nodes. The pace at which changes are recognised, abstracted and communicated conditions the responsiveness of the adaptive risk (re)analysis procedure.

So, the efficacy of analytical procedures and heuristics which are knowledge dependent and employ models of cybersecurity phenomena within organisations is bound by two factors. The first factor is the presence of a technical infrastructure which facilitates the acquisition of necessary data — the second component of March's (2006) 'Technologies of Rationality' triad — as well as its management and sharing. The second factor consists of the cognitive dimension responsible for higher order interpretation (within adequate, dynamic representational models) and subsequent action. These two high-level dependencies correspond with Franke and Brynielsson's (2014) overview of Cyber Situational Awareness as a dual strategic construct which encompasses a technical and a cognitive dimension.

Situational Awareness theory has been established in recognition of the cognitive demands imposed by dynamic, complex systems on decision makers (Endsley 1995). In spite of its initial actor-level conceptualisation, the construct is also used in a scale-agnostic manner in relation to cybersecurity decision-making within macro-systems. This is evident in its explicit role in national cybersecurity strategies (Franke and Brynielsson 2014). Thus, its malleability is attributable to its explicit systemic orientation: "Situation awareness is gained by a system…" (Barford *et al.* 2009:4), and is a "state of knowledge" (Endsley 1995:36) achieved through a series of processes which are described as 'Situation Assessment'. The development of such an epistemic state is central for functional 'sense-making', which further shapes the representation of the operational context, the adaptation of inferential pathways, and the

interpretation of real-time occurrences — all central components of Adaptive (Cyber) Risk Management.

At a high level of abstraction, these processes are consistent with previously described decision-making archetypes. They consist of an epistemic progression through three core steps: situation recognition, situation comprehension, and situation projection (Endsley 1995, Barford *et al.* 2009). Recognition entails framing the situation and identifying relevant elements; comprehension positions otherwise disjointed elements in representational models; and projection is an act of conditional inference to establish action-pathways which lead to the desired outcomes. However, the (Cyber) Situational Awareness perspective presents distinct tools and insights complementary to the emerging Adaptive Cyber Risk Management narrative and supported by the empirical findings of the case-study. These include the centrality of decision makers and the role of cognitive constraints, the spatiotemporal confines of the situation assessment, the nested nature of cyber situational awareness within the larger, systemic situational awareness, and the necessity of fusing and assessing heterogeneous data. From a technical point of view, this entails the establishment of an Adaptive Information System, which can act as a central node, exerting and accommodating epistemic feedback.

The process of data fusion is central to the cyber situation assessment, placing significant emphasis on the role of information systems and decision support technologies. On this point, Franke and Brynielsson (2014:20) note: "Situational awareness by necessity involves both technical and cognitive challenges in that the basic data used for developing situational awareness comprises some kind of underlying estimate of the state of the world which, in turn, is the result of some kind of data processing". As a result, the epistemic transition between scattered data and actionable knowledge is conditioned by information quality, and on the success of the fusion procedure. So, central to the efficacy of projections based on situational awareness lies an understanding of both the validity of data as a descriptive input, and of the completeness/sufficiency of existing situational comprehension. This principle is aligned with the view of Risk as conditioned by knowledge proposed within Bjerga and Aven's (2015) conceptualisation of Adaptive Risk Management. However, the (C)SA view enables expanding the principle through evaluation/validation based on the data, the fusion process,

the representations developed, and (potential) efficacy of inference. Furthermore, a knowledge-network based view consolidates the primacy of epistemic 'fusion' in a central function for establishing and maintaining Adaptive Cyber Risk practices.

An important attribute of modern Cyber Situational Awareness literature is its primarily operational focus. This is distinguished from the arguably broader scope entailed by Adaptive Cyber Risk Management. Network monitoring, operational indicators, sensors, visualisation techniques, and automation algorithms are all envisioned as key sense-making tools necessary for establishing a real time Situational Awareness of the situation (Barford *et al.* 2009). As a 'situation' is manifested in spatial and temporal confines, its understanding is argued to present procedural regularities. In this context, Tadda and Salerno's (2010:17) definition of understanding entails enough knowledge to infer the situation's potential consequences, and predict patterns. From this perspective, the 'cyber' domain is not seen as inherently distinct.

"What is real is the continual change of form: form is only a snapshot view of a transition." (Bergson 1911 in Allen and Boulton 2011:167)

However, both the conceptual framework-derived diagnosis and the in-depth case study challenge the assumption of a sufficient degree of ontological regularity required for achieving such an understanding across scales of analytical granularity within an organisational cybersecurity environment. The efficacy of prediction and pattern forecasting within the domain is inherently conditioned by non-linear dynamics, actor induced variation form model behaviour, capabilities, resources, competing adaptive pressures, lack of adversary specificity, threat vector variety, and 'unknown unknowns'. Given this picture of deep uncertainty, the emerging prescriptive model positions the function of Cyber Situational Awareness as nested within an Adaptive Cyber Risk Management archetype, which enables philosophical consistency. This encourages an explicit critical stance on the local efficacy of inferential outputs, to supplement the validation of inputs and assumptions, in-line with the previously described meta-cognitive analogue function. A high-level overview of this model is presented in fig. 7.

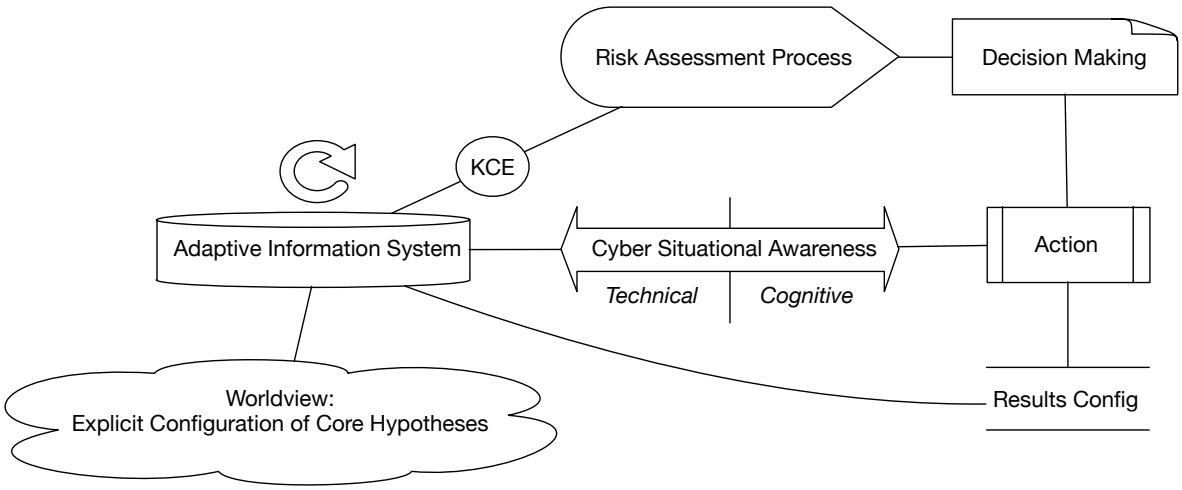


Fig. 7. A high-level view of ACRM

5.2.4 Accounting for Bias in Schema-Based Agents and Structures

Both the case study and the literature-based conceptual framework highlight the necessity of accounting for and mitigating against bias in cyber risk prescription. In spite of heterogenous anecdotal outlines of bias and the variety of theoretical approaches to 'rationality' and its limitations, the case study and the literature present a regularity in defining the construct. As per the literature review, bias entails a contextual failure of heuristic judgements, whereby the (more accessible) heuristic attribute used yields an inadequate representation of a 'judgement object' (Kahneman and Frederick 2002). So, bias represents a situational discrepancy between the heuristic attribute, and the target attribute. Extrapolating on this perspective, bias can occur both as a cognition/agent, and as a social systemic phenomenon, as it entails a failure of schema-based environmental navigation. The two are interdependent, as an actor's role, epistemic grounding, and available action pathways are supported by systemic/network structures and mechanisms. Similarly, these structures and mechanisms are shaped by actors, through intent and coordination. As a result, there are two interacting scales of analysis at which bias as an epistemic phenomenon can be addressed. From the perspective of the participant division used within the data collection strategy, cognitive bias is a concern regarding risk analysts and decision makers involved in the adaptive cyber risk management implementation, while systemic bias is

holistic and includes general actors.

The grounding of cognitive bias in heuristic, often opaque mechanisms is consistent across dual process theories (Kahneman and Frederick 2002) and interactionist/argumentative accounts of rationality (Mercier and Sperber 2011, Sperber and Mercier 2012). These perspectives recognise the essential role of cognitive efficiency imposed by the limitations of human perception, and thus position bias within the domain of heuristic mechanisms. When discussing cybersecurity prescription, the notion of bias is pragmatic. In other words, the trade-off between efficiency and accuracy which results from the unavoidable use of a heuristic attribute to navigate a complex, uncertain situation, can only be evaluated in line with its applied outcomes. Organisations, as hierarchical systems, can present multiple, often competing measures of performance across scales. So, as previously established, locally effective heuristics can be globally maladaptive. Formal decision support frameworks manage the resulting uncertainty through assumptions — implicit, and explicit — as heuristic attributes (Allen *et al.* 2007). These include often intuitive judgements of the situation dynamics, relevant elements, model schemata, as well as epistemic judgments, including differentiating value of competing data streams, perception of knowledge state, and implications of historical performance. As these factors converge, the potential for bias in highly uncertain, complex circumstances, is considerable.

"Objectivity is gained by making assumptions explicit so that they can be examined and challenged, not by vain efforts to eliminate them from analysis." (Heuer 1999:41)

Cognitive (rather than systemic) bias mitigation is presented within the literature (Kahneman and Frederick 2002) as a pluralist objective that generally entails the use of critical reasoning (System 2) to identify errors of judgement, while recognising the potential of heuristic intuitive decision-making in complex environments (Mercier and Sperber 2011, Bingham and Eisenhardt 2011). Practically, implied approaches vary from an argumentative exploration of the judgement, to an investigation of the scope of misused intuition, and the calibration (training) of the implicit heuristic model within a given context (Gigerenzer and Brighton 2009). However, for cybersecurity decision-making, cognitive bias mitigation mechanisms are

conditioned by the efficacy of the pluralist behavioural selection processes, feedback cycles across the organisational hierarchy, and the scope of hindsight bias. The first two factors are interrelated, and address an ability to establish a link between a heuristic output, its local, and its global effects.

Furthermore, Schwarz and Vaughn (2002) highlight the significance and persistence of hindsight bias, whereby knowledge concerning the outcome of an event is integrated within its representational model. This creates the impression of outcome inevitability, coupled with an unjustified belief that the outcome should have been anticipated, and the post-hoc alternation of memories which exaggerate what was known. As a result, causal feedback is distorted, preventing effective adaptation. It is important to note that negative or unexpected outcomes absent erroneous judgement are not a product of bias. Retrospective bias correction relies on an ability to distinguish between general negative outcomes and reasoning flaws.

Within the context of intelligence analysis, Heuer (1999) presents a range of mitigative strategies against such mechanisms/tendencies. These include the establishment of competing hypotheses with a distinguishable epistemic configuration (assumptions, intuition, data) — a technique also found in adaptive management, the subjection of the externalised analytical rationale to collective critique, the selection of context appropriate analytical tools (i.e. lynchpin analysis), and the recognition of common bias tendencies. Once made explicit, epistemic configurations can be subjected to a systematic evaluation of both components and effects. Cognitive bias mitigation can also rely on the relative positioning and architecture of the epistemic network. Attributes like the format, scope, and affective impact (Slovic *et al.* 2005) of the information that is accessible by actors can affect decision-making. These issues were also identified within the case-study, as 'cybersecurity knowledge' has been presented as a construct with contextually varied forms: abstract, in-depth for experts, narrative-based for users.

Similar to cognitive bias, systemic bias entails undesirable collective behaviour patterns and tendencies which result from inadequate representational models or inferential procedures. In principle, this can be corrected by maximising the adaptive architecture of the system

(Benbya and McKelvey 2006a), or by adjusting the relevant inferential configuration. Most of the examples of bias described within the case-study were manifestations of systemic bias, whereby a local heuristic is produced based on myopic sub-system representations. So, potentially conflicting objectives such as the pursuit of cybersecurity and cost-cutting, or openness are misrepresented to favour the locally advantageous heuristic — a phenomenon which can be amplified by structural power dynamics. In this sense, such misrepresentations can only be discussed as erroneous within their systemic context. Furthermore, through the social dimensions of agency (role, norms, culture) globally maladaptive heuristic beliefs can be reinforced and disseminated, becoming a function of the system rather than the actor.

An example of this phenomenon was provided within the context of University X's subsidiary, where the main described source of bias relating to cybersecurity was the organisation's primary orientation for profitability. Such an absolute preference is neither uncommon, nor inherently erroneous for a commercial venture — an essential determinant of bias as a construct. However, the representation of profitability as an absolute priority to an organisation can prove to be locally maladaptive as a source of neglect for amassing vulnerabilities and threat actor presence. If the complex environment of the organisation changes to include other significant threats, a static heuristic preference can indeed lead to systemic bias. Furthermore, in the event of a breach, the effects can be broad, difficult to gauge, and potentially span beyond profitability (Thomas *et al.* 2013). Systemic bias must also be distinguished from Risk Appetite. The latter involves an informed, intentional exposure to risk in the pursuit of an objective, whereas the former is a product of epistemic failures resulting from the system design, its dynamics, and tendencies.

Within the context of Adaptive Risk Management practice, correcting and mitigating against systemic bias involves an ability to link embedded representational models and inferential procedures with patterns of behaviour and outcome variance/deviation. Distinguishing between uncertainty based variance, and inferential error is a highly contextual task, making general prescription challenging. However, by externalising shared intuitions, beliefs and assumptions, a broad range of epistemic validation procedures can be put into place. Instances of externalised inferential epistemic outputs are most notably described by McElroy (2000, 2003) as 'Knowledge Claims'. These are defined as a product of learning, and consist

of "conjectures, assertions, arguments, or theories about which potential actions might lead to desired outcomes" (McElroy 2003:7). Subsequently, they can have a descriptive, explanatory, predictive, or evaluation-centric form (Peters *et al.* 2010). Knowledge Claims are introduced as part of a wider framework — the Knowledge Life Cycle — and are compatible with a collective, relational interpretation of knowledge. Furthermore, in their formulation, they manifest a convergence of available Data, Information, Knowledge and Wisdom for a given situation (Faucher et al. 2008). While functionally congruent with 'competing hypotheses' within Adaptive (Risk) Management, Knowledge Claims benefit both from a robust conceptualisation as an externalised unit of conditional/inherently incomplete knowledge, as well as from an epistemology-derived evaluation toolkit (Peters *et al.* 2010).

5.2.5 Knowledge Claims as Adaptive Triggers

The understanding of action-pathway selection under uncertainty as conditioned by available and emerging knowledge is central to Adaptive Cyber Risk Management. Knowledge Claim validation can occur both passively through positive feedback (McElroy 2003), and actively through Knowledge Claim Evaluation procedures. Both approaches are conducive to epistemic adaptation in response to learning and environmental changes. Furthermore, the evaluation process is presented by Firestone and McElroy (2003) as the key differentiator between information and knowledge. Literary approaches to Knowledge Claim Evaluation are divided based on their epistemological stance. Most notably, Peters *et al.* (2010) identify three core stances: a 'Managerial' approach, centred around justification on grounds established by top management; an 'Entrepreneurial' approach, based on intuitive, coherence seeking validation, at the expense of systematic justification practices; and, finally, an 'Open' approach, based on Knowledge Claim testing through epistemic criteria, which include "logical consistency, empirical fit, systemic coherence, simplicity and heuristic quality", while incorporating procedures of "falsification and error elimination" (Peters *et al.* 2010:251). Amongst its characteristics, the Open perspective is based on a recognition of the untenable nature of absolute knowledge and certainty given organisational dynamics. It also holds authority as an inadequate sole source of truth and a poor substitute for epistemic evaluation.

Amongst the three approaches, Open KCE is both philosophically and prescriptively consistent with the emerging conceptual framework, and complements the critical epistemic awareness. Within the stance, knowledge claims operate as World 3 constructs, able to influence World 2 beliefs (Popper 1978, Firestone and McElroy 2003). Given the emphasis on epistemic evaluation, the progression/evolution of knowledge claims is documented in the form of meta-information (Peters *et al.* 2010). This approach corresponds with Heuer's (1999) mitigative prescription concerning hindsight bias, whereby actions should be traceable to an explicit configuration of epistemic building blocks. Access to a clear link between underpinning knowledge, action and outcome can be used to improve the efficiency of epistemic adaptation, while compensating for cognitive distortion and post-hoc rationalisation. The construct of meta-information is central to the systemic 'meta-cognition' function described in the previous chapters, as it enables the calibration of certainty and the evaluation of localised inferential prowess. Within the Knowledge Life Cycle model (McElroy 2000), the KCE stage can classify Knowledge Claims as Validated, Invalidated, and Non-validated — each position being accompanied with the production of meta-information.

Within the context of Adaptive Cyber Risk Management, the validation status of knowledge claims coupled with the meta-information can be used to elaborate Bjerga and Aven's (2015) Knowledge Strength matrix. It also enables targeted investigation, enquiry and information management, while providing insight into the need for epistemic exploration or exploitation. Heuer (1999) identifies four operations of information acquisition within the context of intelligence analysis. These are: *Additional details about an existing variable; Identification of additional variables; Updated value of existing variables; Information about variable importance and (inter) dependence*. These operations form the basis of an active approach to KCE, whereby non-validated Knowledge Claims can be supplemented, before being subjected to another cycle of evaluation. They also enable consistency in Knowledge Claim formulation as the Open KCE approach encourages the normalisation of competing knowledge claims. This entails ensuring completeness, consistent specificity, continuity with previous knowledge claims (path dependency). (Peters *et al*. 2010)

In spite of its contextual merits, the Open KCE approach also presents a number of epistemology-derived limitations for cybersecurity applications. From a philosophical

standpoint, the commitment to a critical-realist stance centred in truth-seeking can be problematic when it conflicts with organisational pragmatism. Instances of the prioritisation between Usefulness and Truth were highlighted previously based on the literature on the role of cognitive/collective heuristics and systemic exaptation. The teleological function of organisational cybersecurity is one of loss mitigation/avoidance within which its truth seeking functions are nested. This calls into question the assumption of truth seeking as an inherently superior long-term strategy, regardless of context. As a result, ACRM prescription should recognise the role of power-structures, management, and expertise in reconciling conflicting narratives into an actionable worldview. Furthermore, the role of heuristics, intuition and tacit expertise in uncertain circumstances should also be recognised as epistemic drivers. Both of these considerations are exemplified within the case study where the function of leadership in a cybersecurity context is based on the reconciliation of dichotomies. Additionally, analyst intuition was presented as an active driver of prescription, in spite of it not being explicitly described as such within tangible outputs, i.e. risk reports.

The two examples are, however, different epistemic instances. The first involves representational calibration under uncertainty, whereby leaders reconcile potentially conflicting representations of reality. This is indeed a truth-seeking operation and involves competing Descriptive/Representational Knowledge Claims (DKC). Even when subjected to a Managerial KCE approach, such an operation involves socially moderated epistemic validation. In contrast, the latter exemplifies an instance of predictive inference based on existing Descriptive Knowledge Claims. The resulting 'Risk Knowledge Claim' (RKC) is usefulness oriented, and can be subjected to heuristic assessments, i.e. contextual ecology/adaptive toolbox. However, unlike its counterexample, it is inherently incomplete, conditional and probabilistic, describing eventualities, which limits the utility of grounding epistemic validation solely in terms of truth through tools like falsification, simplicity and continuity. This distinction is meaningful as it enables a two-layer validation within the risk assessment process based on the type of the Knowledge Claim. DKCs require the primarily truth-oriented validation associated with Open KCE. This includes a description of known-unknowns, uncertainty, and descriptive limitations as it emerges in the form of meta-information. However, RKCs must explicitly account for analyst intuition/expertise as a source of procedural variation, managerial concerns and performance criteria, local risk mitigation

ability, and heuristic context. In simple terms, DKCs must be true, while RKCs must employ DKC configurations usefully.

5.2.6 Knowledge Claim Parameters: Adaptive Risk Quantification and Meta-Cognition

A foundational prerequisite of selection-based adaptive strategies is the ability to distinguish contextually successful units of adaptation (March 2006). Managing Knowledge Claims as adaptive units enables the homogenisation of the various epistemic streams (Threat Knowledge, Business Knowledge, Mitigative Knowledge) into a consistent output, with a modular, relational structure. In addition, a Knowledge Claim-oriented Adaptive Information System can incorporate Benbya and McKelvey's (2006a) first principles of adaptivity. These include: the maximisation of positive feedback by adjusting the weight of various inputs based on recorded inferential performance histories; the identification of adaptive tensions, as made visible in the knowledge claim formulation, normalisation and evaluation procedures; the inclusion of variation by design in competing interpretations of data; and the pacing of KC production-evaluation-adaptation loops based on changes in the representations, as identified through the CSA function. Validated KCs can also form the basis of collaboration within the epistemic network. Through a normalisation procedure, inter-organisational KC conflicts can be directly explored as a potential source of feedback. Finally, a re-emerging theme within the case was the difficulty caused by unknown unknowns. Within the proposed models, the pragmatic scope of the unknown resides in the gap between expected and actual inferential performance. As a result, the granularity of effective prediction/projection can be assessed and accounted for in both spatial and temporal parameters.

Maximising knowledge claim adaptation within the proposed approach to cyber risk KCE raises the issue of structural differentiation. Firestone and McElroy (2003:152) identify 24 types of 'Knowledge Claims', which range from factual statements, to application software, data models and methods. Within the current context, these are seen as inputs/modules for Descriptive Knowledge Claims, or Risk Knowledge Claims, based on their function and scope. For example, a descriptive, threat-based knowledge claim entails structural coherence

through a range of potential inputs which include data, models, and statements. Because of its composite nature, structural modularity, and its associated meta-information, it can be compared with competing knowledge claims that are built on different inputs, or are a function of different nodes in the knowledge network. Subsequently, KC structural archetypes are central to the functional integration of KCE within an Adaptive Cyber Risk Management framework. Furthermore, in the proposed interpretation of Adaptive Cyber Risk Management, KCE is distinguished from CSA-based data validation and information production, outputting epistemic structures able to adapt based on heterogenous feedback. This proposed sequential evaluation process is illustrated in fig. 8.

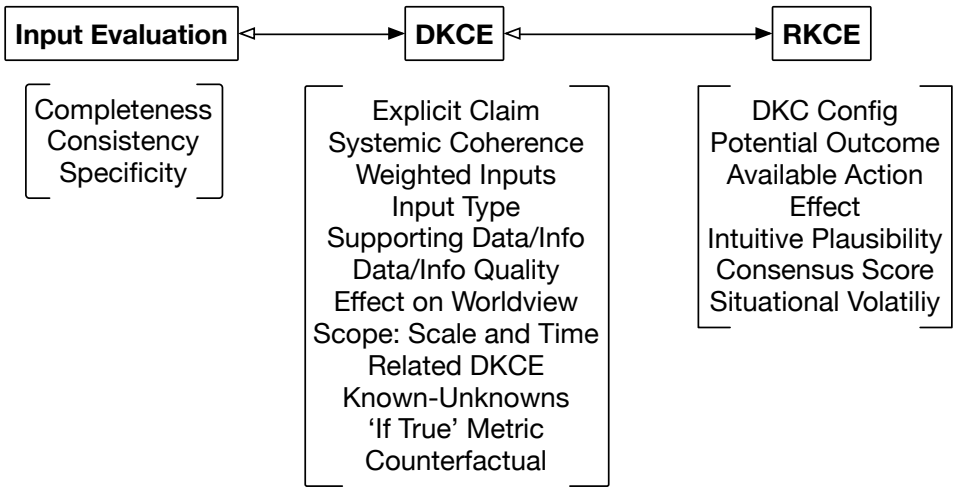


Fig. 8. The Adaptive Cyber Risk Knowledge Claim Evaluation Sequence

As RKCs aim to represent contingencies which vary in likelihood, complexity and scope, cyber risk quantification consistency — an issue raised in both the case and the literature review — must explicitly incorporate measures of systemic 'meta-cognitive' awareness. This entails an understanding of both representational model accuracy/truthfulness, achievable through KCE, and of the procedural efficacy of projection/inference through available DKCs at various degrees of granularity. In other words, decreasing cyber risk analysis subjectivity/variability entails a procedural evaluation of how accurate the claims describing the organisational reality are, and of how well these descriptions can be used to infer patterns of likely behaviour. Based on the process of knowledge claim normalisation, whereby competing knowledge claims are structurally consolidated, metrics can be introduced for core evaluation categories, each holding trainable weights based on historical performance.

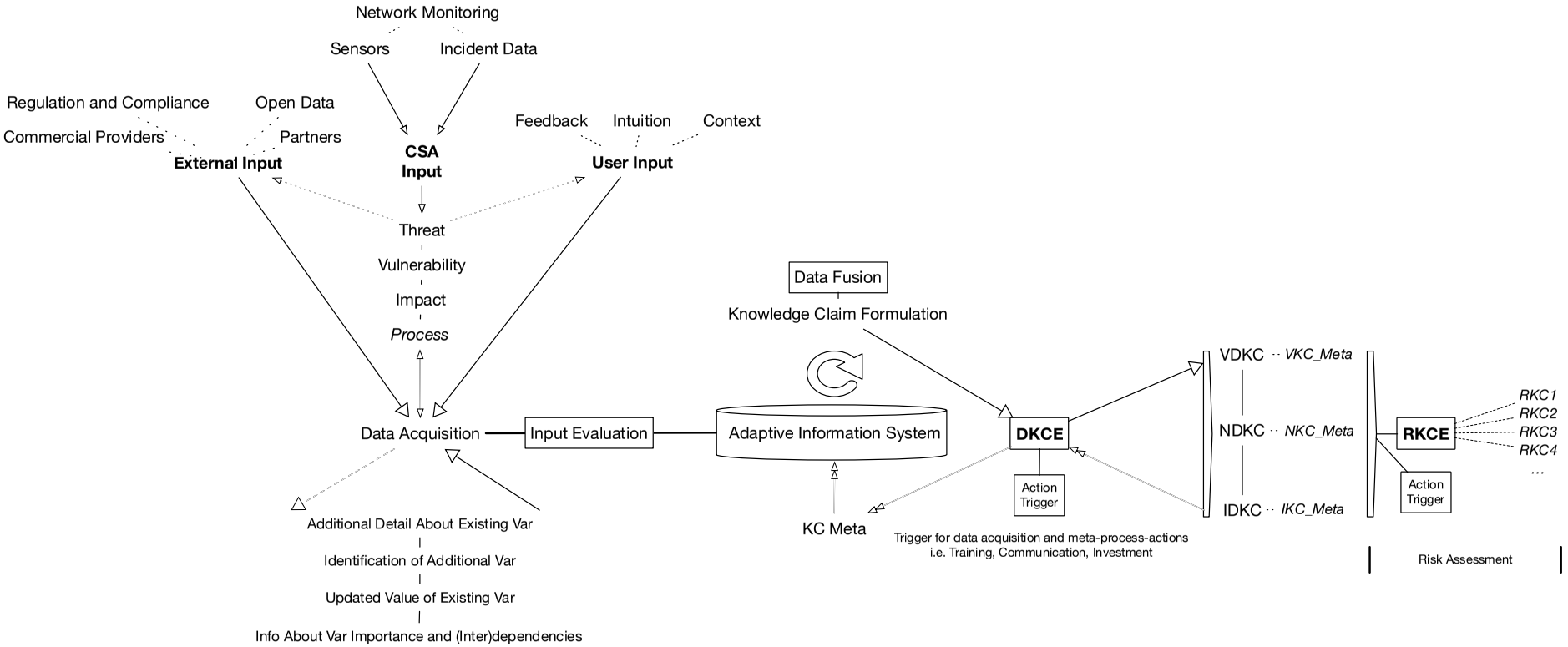
As a result, informational inputs can be distinguished based on locally established evaluation parameters like their type, source, and the degree of systemic coherence they present (a broader range of such parameters is proposed in fig. 8. Through positive feedback, high performing inputs can benefit from a proportionally increased weight in the KCE process. By gradually expanding and adapting the base of DKCs employed, the worldview addressed through the risk process evolves.

Furthermore, having access to such an explicit configuration of support parameters for competing knowledge claims enables mitigation for hindsight bias, provides a critical understanding of the epistemic conditionality of specific risk claims, and maximises the utility of post-incident feedback/calibration. The dual KCE process also enables organisations gauge both their descriptive and, respectively, their inferential ability within a cyber risk setting. A low confidence DKC-base can be an indicator of necessary adjustments to sense-making strategies and infrastructure. Similarly, the degree of systemic uncertainty can be extrapolated based on the relationship between RKCs and their supporting DKCs. Once the scope of complexity-based uncertainty is established, further strategies for uncertainty mitigation can be implemented at each relevant level of analysis. A visual representation of the proposed framework which incorporates the proposed Adaptive Information System is provided in fig. 9, based on an expanded view of the previously introduced Adaptive Cyber Risk meta-model (fig. 7).

The visual model expands on the sequential evaluation process within the context of the ACRM meta-model. In addition to providing a core taxonomy of inputs relating to the Threats-Vulnerabilities-Impact triad, as well as process related data/information, the model introduces the information acquisition function predicated on Heuer's (1999) classification. Acquired inputs are evaluated and introduced into the Adaptive Information System where the CSA-derived Fusion proceeds — a precursor to knowledge claim formulation. Initially, Descriptive Knowledge Claims are evaluated, and classified into Validated, Non-validated, and Invalidated Knowledge Claims, as per McElroy's (2000) Knowledge Life Cycle model. As part of the DKCE process, actions, such as using the data acquisition function, or acting on descriptive insights, are enabled. In addition, the distinct epistemic configuration and meta-information of each evaluated knowledge claim is fed back into the Adaptive Information

System, shaping future iterations of the process. Finally, Risk Knowledge Claims are made primarily based on configurations of validated Descriptive Knowledge Claims. Again, through the RKCE process, actions can be triggered. Finally, following their evaluation, the validated RKCs form the basis of Risk Assessment, being reviewed and updated based on changes in their underpinning assumptions, inputs, and supporting evidence. Given the relational nature of this progression, the implications of downstream (i.e. core data/information) changes can be highlight the necessity of updating the relevant Knowledge Claims. Based on use efficacy and local best-practices, the pace of feedback cycles can be optimised to match the dynamics of the targeted level of analysis.

Fig. 9. The Adaptive Information System Architecture:



5.2.7 Formalising an Epistemic Framework for ACRM

Throughout the previous sections, Adaptive Cyber Risk Management was introduced as a versatile prescriptive framework/conceptual archetype which can address the core requirements and considerations raised through both the literature review and the case study. Most notably, these include the high-uncertainty and environmental dynamics presented by the cyber domain, a low efficacy of static system models, a potentially high level of agency-induced systemic variation, and a need for effectively engaging local epistemic networks. However, given the relative novelty of applying Adaptive Risk Management within cybersecurity, several considerations were raised. These include the necessity for positioning the framework in a systemic context, where the utility of the implementation is conditioned by epistemic processes and (technical) infrastructure, as well as by cognitive, analyst related dimensions. Both the temporal sensitivity of adaptive triggers and feedback, and the effects that it has on risk models highlight the importance of real-time sense-making capabilities and situational awareness. These points were addressed through the incorporation of Cyber Situational Awareness theory as a complementary construct which places emphasis on the technical dimension of data-collection and interpretation, on the implications of agency, and on real-time response capabilities.

In addition, the 'Knowledge Claims' construct was introduced as a unit of epistemic adaptation. As per Bjerga and Aven's (2015) conceptualisation of ARM, risk is used to quantify heterogenous epistemic events. An ability to understand and represent epistemic differences between Knowledge Claims is central to a more nuanced description of Risks. This ability is supported by a contextual formulation of Knowledge Claim Evaluation processes, which allow Knowledge Claims to expand the function of hypotheses in Adaptive Management, by distinguishing appropriate validation tools based on the function of they hold. They also enable the incorporation of adaptivity maximising approaches, such as Benbya and McKelvey's (2006a) first principles of adaptation. Once validated, defined in scope, and prescriptive utility, Knowledge Claims can serve as a malleable foundation for communication and collaboration strategies, as they can be transposed in the form of narrative, or in the form of data-inputs, based on use-case. The 'open' approach to DKCE also enables user

input/feedback from across the hierarchy for the formation and adaptation of internal/business representational models, used to establish vulnerability and impact assessments. Finally, the framework also enables the retrospective use of competing heuristic approaches, and risk quantification methods as a historical record of available knowledge (claims) is generated.

Through the above, the framework prescriptively addresses the context-construct gap diagnosed in the earlier chapters of the thesis, while also better equipping organisations to locally deal with the epistemic challenges of cybersecurity as a knowledge-problem. More specifically, the (meta-)framework is predicated by an awareness of the relational knowledge networks predicating knowledge in cyber risk management by acknowledging and leveraging the role and attributes/requirements of epistemic nodes in the production of units of adaptation (knowledge claims). It also proposes a technical infrastructure for epistemic convergence, feedback maximisation, and selection in organisational sensemaking. The potentiality and the effects of deep uncertainty are also central to the framework, which incorporates adaptive mechanisms underpinned by processes for distinguishing between epistemic operations (description and inference), for retrospective procedural and representational calibration, and for a 'meta-cognitive' awareness of the environmental uncertainty faced. At an axiomatic level, a nuanced level of 'rationality' is used, which enables the identification and recognition of the potential causal role presented by multi-granular 'soft' dimensions of social systems, like cognitive tendencies and mechanisms, incentives and culture within cyber risk practice. By doing so, the conceptualisation/formulation of Adaptive Cyber Risk Management put forward presents promising novel avenues for both research and practice in organisational cybersecurity management.

5.2.8 Framework Development: A Commentary

As a product of its preceding stages of analysis, the Adaptive Cyber Risk Management framework aims to embed a series of systemic and epistemic mechanisms under an organisational risk paradigm. Its development relies on the explicit recognition of adaptivity as a necessary attribute in a cyber risk context. This is supported by the claim that the estimations of likelihood and impact for potential cybersecurity events in a specific systemic setting are conditioned by knowledge, and are primarily used to trigger adaptive responses. Moreover, the framework attempts to address systemic non-linearity and behavioural dynamics in a coherent manner, as persistent yet underrepresented drivers of organisational cybersecurity outcomes. The development of the framework in response to the theoretical and empirical findings of the study (as described in sections 5.1 and 5.2) loosely follows three stages. Firstly, the baseline meta-structure is identified, which grounds the framework objectives, and its structural/operational logic. Secondly, the a high-level overview of the core functions that are necessary to achieve these objectives is provided. Thirdly, a more in-depth perspective concerning the epistemic structure of the framework is developed, which aims to mitigate against behavioural (i.e. biases) and systemic (i.e. stochastic uncertainty) tendencies affecting efficacy of risk analysis/management.

The baseline structure of the framework is derived from its positioning at the intersection of technologies of rationality and adaptation seeking strategies. This entails a preservation of the simplified structure of the former — i.e. basic relational models of the problem, data, and decision rules — while placing additional emphasis on the basic conditions for adaptation: reproduction of success, and generation of variety. Such a structure enables the framework to be compatible with existing risk guidelines and standards (a necessity, given the highlighted organisational reliance on risk as a paradigm), while also providing avenues for methodological novelty. Adaptive Management derives from a conceptual lineage positioned at this intersection, balancing structured, model-based outcome anticipation with an embedded adaptation seeking mechanism.

While traditionally associated with complex environments and deep uncertainty, the literary presence of Adaptive Management does not directly address the challenges

presented by organisational cyber risk, nor does it place particular emphasis on the social dimension of systems. It does however provide a blueprint for epistemic adaptation through model/claim variation (competition), selection, and success replication. In spite of the absence of a clear theoretical lineage, Adaptive Risk Management (the convergence between Adaptive Management and Risk Management) emerges as a flexible, balanced perspective, which places emphasis on the epistemic conditionality of risk claims — i.e. event identification, likelihood and impact estimates. The lack of a widely accepted interpretation of the concept (ARM) also presents opportunities for accommodating compatible observations and findings from the previous chapters.

Most notably, in a centralised risk analysis/management function, risk profile/posture adaptation is not directly triggered by relevant environmental changes, but by specific informational exchanges concerning said changes. In addition, the cyber risk function employs a relational knowledge network in order to develop adequate representational models. Furthermore, models in a risk setting are discrete representations of continuous cross-hierarchy systemic interactions. Subsequently, their adequacy is constrained by spatial and temporal attributes which underpin both their adaptive tension, and the overall sustained adequacy of the practices which they inform. And, operationalising an epistemic perspective must account for knowledge as a structurally moderated trigger of action (i.e. can be subjected to a usefulness continuum in a given setting, based on the fitness of resulting actions). Finally, following the systemic complexity framing suggested by the literature review and the case study, adaptive heuristic formulation to identify and exploit manifested ontological demi-regularities can prove to be an effective strategy, even in the absence of complete system models. As a result, this first stage of framework formulation provided a foundation of assumptions and desired outcomes, following the theoretical analysis and the case study.

The second stage of the framework formulation process consisted of constructing a model of core functions which can accommodate the necessary information architecture/exchanges in an Adaptive Cyber Risk Management implementation. This broadly entails building upon a relational information flow model which covers Framing, Input, Analysis, Decision, Action and Outcome as discrete functions shared by main risk management methodologies (Appendix

5). These generic functions are adapted in order to maximise adaptive potential and support bias mitigation/heuristics formulation techniques. So, the framing function manifests an explicit configuration of assumptions — a world view — which serves as a foundation for the identification and reproduction of adaptive success. As competing knowledge claims with modular, formal epistemic validation structures are used to inform decision-making, the outcomes they are linked to, and the framing assumptions that they are based on must both be individually identifiable as a pre-conditions for replicating adaptive success.

The explicit link between framing - claim - decision - outcome (relying on the proposed adaptive information system/knowledge claim evaluation sequence) is a prerequisite for an ability to gauge the adequacy of the underpinning worldview, and to engage in the retrospective calibration of each function in a manner that mitigates against hindsight bias. Furthermore, it enables a systemic interpretation of the 'adaptive toolkit' for heuristic formulation. Another primary dimension of the high-level view of the framework is the integration of Cyber Situational Awareness as a concept. Through its technical and cognitive dimensions, it is able to provide a balanced perspective on the pre-requisites for developing and maintaining a systemic state of awareness. This is achieved through a representational schema that accounts for both infrastructural/technological and cognitive/behavioural dimensions of uncertainty navigation in a cyber setting. From a framework perspective, a functional representation of cyber situational awareness has a dual role: it introduces a potentially real-time feedback meta-function, based on the inputs of the technical infrastructure (i.e. sensors, firewalls, network monitoring capabilities); and, through the concept's substantial literary presence, it provides procedural and technical guidance for developing and improving such a systemic state of awareness. Finally, through its perspective on data fusion, the CSA perspective influences the formulation of the Adaptive Information System component as a prerequisite for centralised risk model formulation and coordination. By doing so, it provides a structure for the epistemic progression between data, information and knowledge claims, and it is able to accommodate a variety of mechanisms and strategies which support the framework's objectives.

The third stage of the framework formulation process consisted of building upon the emerging structure and relational logic, to maximise epistemic adaptivity, mitigate bias and

implicitly improve heuristic formulation/adaptation, while also adding an additional dimension to the risk claim generation function. This has leveraged the knowledge perspective of the study, introducing stage appropriate evaluation and validation procedures throughout the epistemic progression between raw data and risk knowledge claims. Emphasis is also placed on the knowledge claim formulation and evaluation processes, where the meta attributes resulting from each stage (i.e. classification of knowledge claims as validated, invalidated or non-validated) are used as feedback points reinforcing epistemic inputs, formats and fusion procedures. At each stage, this feedback can be used to trigger the information gathering functions, while also calibrating the evaluation practices, and providing aggregate indicators concerning the coherence and adequacy of the risk framing foundation/worldview. The combination between these operations, inputs, and attributes serves as a foundation for the modular knowledge claim configuration proposed to achieve adaptive epistemic strategies (introduce variation, and identify/replicate success). Through the literature on knowledge claim evaluation approaches, the descriptive and inferential dimensions of risk analysis were identified as interlinked yet distinct. This presents an ability to distinguish between the descriptive efficacy of the representational models informing the later stages of risk analysis, and the utility of subsequent inferential procedures relying on specific configuration of descriptive knowledge claims, which serve as the output of risk analysis. As a result, the relationship between the descriptive and inferential dimensions of risk analysis can be evaluated from the perspective of specific outcomes, as a basis for adaptive efforts.

While the mitigation of specific cognitive biases derived from the literature review, i.e. hindsight bias, is explicitly addressed by the previous chapter, the framework more generally addresses bias as a failure of heuristic attributes, both at a systemic and a behavioural level. As a result, mitigation is seen as a function to identify heuristic failures at the level of specific epistemic operations, and relies on an adaptive mechanism able to generate alternatives (variety), while leveraging positive feedback. An important emergent function of the additional epistemic layer proposed by the framework, is described as a meta-cognitive analogue — an epistemic awareness of inferential acumen/performance able to distinguish between inherent uncertainty and procedural and, more broadly, informational failures. Through the introduction of lifecycle specific epistemic metrics which feed into the CSA and

the Framing functions, anomalies, expected performance levels, and improvement areas can be highlighted in a contextually anchored, evolving manner. As a result, the Adaptive Information System model, through its explicit system of knowledge claim encoding and evaluation, can be used to support, assess, and adapt the efficacy and scope of knowledge-sharing practices throughout the epistemic network, while framing the performance of the cybersecurity function in a wider organisational context.

5.2.9 Framework Implementation Applicability

Despite the fact that the previous chapters have addressed the framework from a primarily theoretical/conceptual perspective — i.e. a step removed from implementation — the potential implementation-level applicability of the proposed interpretation of Adaptive Cyber Risk Management has also been considered throughout its stages of development. This will be briefly explored in three dimensions: *Compatibility* with existing frameworks and guidelines; *Flexibility* to varied organisational settings; and, *Utility* at an implementation level. It must be highlighted that the following is structured as a commentary. Subsequently, it aims to clarify and support the previous sections, and reflects the researcher assumptions and intentionality at the time of writing. Each of the points raised can potentially be subjected to amendment as a result of follow-up empirical work.

From a compatibility perspective, the framework was constructed to support, supplement, and expand the scope of existing risk management practice. As a result, it avoids rigid methodological prescription and highly context-specific guidance, while also avoiding emphasis on Cyber Risk Management areas which are either not directly affected by the theoretical/empirical findings (i.e. risk treatment strategies), or are exhaustively covered by industry standards (i.e. threat/risk taxonomies, likelihood evaluation approaches). Furthermore, through its conceptual framing (Panarchy/hierarchical coevolutionary organisational-environment relationship) the output shares the definition of cyber risk, and its nested character within enterprise risk with the major industry standards covered in Appendix 5. Through its functions, the framework enables both the ISO/IEC (2018) and the NIST (2012) risk management process, while expanding the speed, scope and structure of the

inter and intra process feedback. And, while it has not been a focus of the study, the framework and its underpinning theory could assist with managing other, similarly volatile dimensions of enterprise risk in a holistic manner. Given its mechanism-oriented formulation process, the framework is designed as a guide rather than a rigid structure to adhere to. As a result, in addition to a functional overview, it provides direct references to additional supporting documentation and literature for each construct it employs (e.g. Cyber Situational Awareness). While limiting the depth of prescription, this non-specificity enables greater implementation level flexibility, and avoids a potentially restrictive interpretation of key concepts.

Given its mechanism-centred approach, the framework is relatively context agnostic. While the scope of a potential implementation is indeed likely to be largely shaped by its specific organisational context (scale/structure/operational model), the functions and their relationships are seen as broadly applicable, assuming a susceptibility to cyber risks, and a formal risk management process. So, a limited version of the framework can be implemented even in organisations which are either small, or operate in a low hostility cybersecurity climate. In such settings, the use of Adaptive Cyber Risk Management proposes the integration of adaptive mechanisms, an systematic approach to support cyber risk centric communication, and the development of a formal approach to gauge the sustained validity of framing assumptions and representational models. Thus, it can mitigate against changes in threat climate and operational model, while also providing the means to gauge decision maker bias/shared representational model adequacy on the topic of cyber risk. It should be noted that this is a point of conceptual departure from the interpretation of Adaptive Risk Management found in the NIST Cybersecurity Framework (2018), where the term is used to denote the top implementation tier, and is thus applicable to a subset of the organisational population. While not in direct conflict, the proposed interpretation of the term entails a mechanism for bias and (domain) complexity mitigation through adaptive epistemic structures, which aim to highlight the effects of ‘unknown unknowns’ and support the sustainability of existing risk practices. Thus, they support a dynamic understanding risk appetite, and decrease the potential scope of incidents due to unforeseen, inadequately assessed, or changing risks. Subsequently, when combined with a flexible formulation, the proposed framework is seen as widely applicable to a variety of organisational contexts, as it

accommodates variety in the scope and structure of each interpretation.

Finally, the implementation-level utility of the framework has been argued for throughout section 5. A summary of the main points raised so far includes: an explicit set of strategies and epistemic functions to address the highlighted domain specific complexity; an adaptive mechanism supported by an explicit emphasis on input-process-outcome epistemic configurations which underpin the targeted variation, and success replication efforts required; a process for heuristic formulation and calibration/adaptation through positive feedback, which addresses bias at both a decision-maker and at a systemic level; an transition towards explicit heuristic formulations, emergence and coevolutionary hierarchies for both explanatory and inferential operations, better informing decision makers. Based on its theoretical underpinning, the framework plays a direct role in building contextually adequate assumptions about 'rational' actors in risk analysis, from a dual perspective — as decision makers, and as causal drivers of incidents/systemic behaviour. More broadly, it provides an evolving procedural structure which identifies high-performing epistemic configurations and pathways through positive feedback. This presents users with an ability to reinforce organisational learning efforts with a systematic history of the relationship between outcomes and epistemic configurations, including specific sources, interpretations, data fusion procedures, and so on. Finally, given its reliance on positive feedback and explicit epistemic progression pathway reinforcement, aspects of the framework could benefit from automation and machine learning/artificial intelligence (i.e. KCE validation and formulation criteria/configuration selection through machine learning). As a result, the study could contribute towards the development of novel technical solutions to support organisational cyber risk management efforts.

6. Conclusion

6.1 Objectives and Findings

Organisational cybersecurity is a multifaceted, trans-disciplinary, emerging domain of academic enquiry with distinct attributes and challenges for practitioners. Amongst the latter lie under-explored epistemic barriers that are specific to the domain, and affect construct-assisted foresight and adaptation efforts. The previous chapters have aimed to critically explore this premise as a rationale for enquiry that was formulated through two interacting structural/heuristic metaphors: the cybersecurity 'context-construct gap', and the 'knowledge-problem'. This has entailed a theoretical analysis of the research context as the basis for building the conceptual framework (sections 1 and 2), an empirical investigation consisting of an embedded critical realist case study (sections 3 and 4), and a prescriptive dimension where the emerging narrative is used to conceptualise an Adaptive Cyber Risk Management framework in response to the identified problems (section 5).

The research objectives are also approached in a structurally clustered manner and support the overarching aim through the three dimensions: theoretical, empirical, and prescriptive. Objective '0' was met through the theoretical analysis/literature review conducted in section two, resulting in a multi-granular conceptual framework which also informed the nature, logic and topics of enquiry. Objectives 1 and 2 were both met through the methodology chapter, which enabled grounding the scope of empirical enquiry in an explicit philosophy and developing a conceptually-consistent research strategy, and through the multi-level embedded case-study. Subsequently, the case data enabled the calibration/validation of theoretically postulated mechanisms, while also indirectly providing an empirical grounding to the 'knowledge-problem' and the 'context-construct' heuristics. Finally, through the theoretical and empirical foundation of the study, objective 3 was addressed in Section 5, in the form of a novel framework for Adaptive Cyber Risk Management that is predicated on context-specific dynamics and mechanisms.

6.2 Contribution and Implications

The study's contribution to knowledge is primarily theoretical, with significant practical implications. Firstly, it addresses a literary knowledge gap for phenomenon-based, trans-disciplinary theory which converges with empirical findings as the basis for prescription in organisational cybersecurity. In this sense, the heterogeneous conceptual framework provides an early theoretical contribution towards developing a multi-granular conceptual toolkit which can advance enquiry within the field. Due to the attributes of the case setting, the availability of context data, the plurality of perspectives captured, and the efforts made to represent event hierarchy/verticality, the case itself provides an arguably important empirical contribution towards the organisational cybersecurity literature. Given the relative novelty of cybersecurity as a meta-technical area of organisational concern and academic study, the research is among the first which aims to address the inferential dynamics of the domain through multi-level, in-depth case-work. Furthermore, the merits and implications of an epistemic view of organisational cybersecurity have been argued throughout the thesis, which serves as an initial contribution in this line of enquiry. Most notably, it enables going beyond the 'human' and the 'technical' dichotomous division of cybersecurity management, towards a holistic direction where the emergent potential of the interaction between these two aspects is addressed through an epistemic common denominator.

Secondly, from the perspective of its main heuristic/structural metaphors, the study presents a diagnosis and a bottom-up organisational cybersecurity-specific analysis of the 'context-construct' gap. In this sense, it goes beyond previous efforts of acknowledging the significance of systemic complexity in cybersecurity, or the extent of the behavioural variability presented by actors for inferential constructs. Instead, it provides an integrated approach rooted in a series of ontological mechanisms which are found to be significant in driving domain dynamics and tendencies. Given the modularity and the explicit chain of inferences presented by the conceptual framework, it presents a promising, malleable theoretical foundation for novel avenues of analysis to underpin cyber risk research.

The organisational 'knowledge-problem' is also explicitly targeted through the proposed conceptualisation of the Adaptive Cyber Risk Management framework, which aims to maximise epistemic adaptivity, develop a functional 'meta-cognition' analogue, increase the responsiveness to time-sensitive positive feedback streams, and enable knowledge operation differentiation (i.e. description vs. prediction) in a manner that can be calibrated to both the resources and the levels of uncertainty faced by individual organisations. Thus, through Adaptive Cyber Risk Management, additional epistemic vectors for the measurement of competing risk eventualities are integrated in the analytical process in a manner that is locally adaptive and suited to the variability and heterogeneity of cybersecurity events. This presents an opportunity for a more nuanced representational system of cyber risk which can evolutionarily select for locally fit information streams, heuristics, practices and procedures, while also illustrating potential deficiencies in inferential performance.

Organisational cybersecurity management practice can also benefit from the functional framing and findings of the case-study. By providing a clear link between problem diagnosis and framing, postulated explanation, empirical description and inferred prescription, the proposed Adaptive Cyber Risk Management framework can accommodate additional investigation, inputs, and setting-specific adaptation efforts. Finally, the applicability of the findings is rooted in their mechanism-oriented generality. This means that the framework can be operationalised in a wide variety of organisational settings by adjusting it to the local manifestation of its underpinning mechanisms. It should be noted that while the proposed interpretation of Adaptive Cyber Risk Management is practice oriented, its formulation within the context of the study was not geared for direct implementation. Instead, the link between arch-structures, components and mechanisms was emphasised, which entails a higher degree of abstraction than a methodological, practitioner-oriented framework.

6.3 Limitations and Further Study

In spite of the significant levels of institutional support and access made available for the study, some pragmatic constraints were faced due to the nature of the project. Given the role of doctoral structures and processes, the research was conducted under defined

operational boundaries, including duration, scope, and resources. Such constraints are both unavoidable and, in this context, potentially useful for defining the boundaries of the investigation. Concerning the research outputs, as the trade-off between abstraction/generality and implementation specificity is inherent given the nature of the knowledge-gap addressed by the study, an emerging operational limitation is that the scope of the framework is a step removed from practice. This also presents an opportunity for further developing Adaptive Cyber Risk Management in a manner that is directly addressed to practitioners. In addition, methodologically, the single in-depth study can be supplemented with comparative case data as an opportunity for additional testing and calibrating the outlined mechanisms, while exploring their implications in various operational settings. The study also presents technological development opportunities for products/applications, i.e. to support the Adaptive Information System architecture suggested by the framework. Beyond the broad conceptual fit, gauging the feasibility of the output as a foundation for adaptive cyber risk management technologies requires further study.

Generally, the proposed direction of enquiry — a phenomenon-based view of organisational cybersecurity management, and the subsequent role of ACRM — requires additional perspectives on the descriptive claims put forward, and on the comparative pragmatic value derived from the study's prescriptive outputs. The former entails a conceptual exploration of the study's core framing and premises, and their descriptive merits, i.e. representational fidelity of the organisational cybersecurity function as a dimension of a systemic hierarchy. Most notably, this would benefit from a shift in the context of the study by exploring the merits of the explanatory lens in varied organisations, sectors and even nations. Such a pluralistic perspective could introduce dimensions of analysis aiming to strengthen the generalisability of the theoretical framework. In contrast, the latter entails an implementation-level evaluation of the principles put forward. This raises an emerging research area: bridging the framework's current conceptual form, and an application-oriented interpretation. More specifically, valuable implementation-level contributions could be made addressing operational context-dependencies such as: considerations for context specific compliance with regulatory bodies and standards; gauging the local effects of variables such as organisational scale, operational model, and macro context; establishing

the compatibility with wider governance frameworks; identifying emerging barriers and implementation difficulties; and presenting potential emergent limitations of an ACRM implementation.

A direct structural/methodological implication of the approach used to develop the Adaptive Cyber Risk Management framework is the absence of an explicit post-formulation validation stage (an issue also discussed in section 3.3.3.5). This is a product of several interacting dimensions of the study, which include the relationship between the theoretical analysis and the empirical investigation, the philosophy, and the attributes of the area of enquiry. More specifically, the case-study supplements the initial literary/theoretical analysis as a process of empirical exploration, calibration and validation of axiomatic assumptions and macro observations. However, the subsequent framework does not attempt to resolve a setting-specific problem, and instead is predicated on the case-moderated conceptualisation of interacting mechanisms as a source of validity. While the mechanism postulation process used to link the case data to a non-case specific framework is compatible with the research philosophy and methodology, it presents a potential point of wider contention and can be seen as a significant limitation. Indeed, the line of reasoning is not one of generalising the anecdotal, but of inferring mechanisms based on the intersection between macro-tendencies, theory (both covered in the literature review), and an exemplary case. Thus, neither the explanatory model nor the proposed framework result solely from the case study, and neither exclusively address case-specific dynamics. Subsequently, case participants provide at best a limited vector of prescriptive validation. Furthermore, establishing the (non-inferred) pragmatic 'validity' of a heuristic construct entails evaluating its comparative implementation performance. This introduces a series of causally significant variables/contingencies ranging from the attributes of the implementation, to the orientation of the framework, epistemic attributes of the events faced, metrics of performance, and the comparative baseline expectations. Such practical challenges to experimental design are common in real world settings, and while they exceed the pragmatic boundaries of the thesis, they also present an opportunity for follow-up research.

Finally, given the cross-disciplinary approach taken, some of the key terms used throughout the study could cause potential confusion due to a variation in their contextual meaning. For

example, terms such as ‘adaptive’ (cyber risk management) are used in accordance to contextually defined parameters, in the absence of a monolithic conceptual lineage to adhere to. While efforts have been made to ensure a theoretically rigorous interpretation of adaptive mechanisms within the context of Cyber Risk Management practice, the term ‘adaptive’ could conceivably be used as a methodological qualifier which indicates different dimensions than those suggested in earlier chapters — particularly under the colloquial interpretation of ‘adaptation’. In light of this, efforts have been made to identify and address such instances in relation to the interpretation used within the project (e.g. In section 5.2, where preceding, varied literary interpretations of ‘adaptive risk management’ are briefly described). This same multi-disciplinary approach presents opportunities for methodological advancement in cybersecurity management. Based on the research framing, there is a methodological opportunity at the intersection between complexity studies and behavioural sciences . This convergence point presents methodological avenues which, while not deemed appropriate or feasible for the current study, are promising and potentially innovative in addressing organisational cyber risk questions. For example, this includes the potential of integrating experiments for agent-level insight, and agent-based models for exploring systemic tendencies and emergent trends in Adaptive Risk Management problems.

6.4 Research Journey

The attempt to engage the topic of organisational cybersecurity management in a flexible manner across disciplines, scales, and frames of analysis has yielded a tumultuous journey. As the discipline-agnostic nature of the research problem became clear, establishing an adequate methodology able to capture and engage the applied manifestations of the core constructs and mechanisms has involved many cycles of trial and error. Unsuccessful iterations have included attempts to explore the dynamics of the problem through techniques ranging from Agent-Based Modeling, which is native to Systems/Complexity science, supplemented by behavioural questionnaires, to a Soft Systems Methodological approach in a critical infrastructure setting. While all (except one) have at least partly failed to yield the desired output, each iteration of the research narrative is in some way embedded

into the thesis, having brought to light new issues and aspects which, once addressed, became part of the subsequent problem framing.

Another significant challenge has been the construction of a heuristic structure able to support and communicate the potential complementarity of otherwise heterogenous constructs. The need summarise to stakeholders how an epistemic focus of organisational cyber risk management must also account for a behavioural dimension introduced by 'rational' actors in socio-technical systems, and for the patterns, tendencies, and attributes introduced by the complex interaction dynamics within said systems has placed significant pressures for the selection of efficient language, constructs and metaphors. Again, through trial and error, some ways of framing the narrative presented themselves as more effective than others. Similarly, while the conceptual lenses used to discuss the research problem have initially introduced a large number of associated constructs, as the project matured, most were eliminated.

The logic of a 'knowledge problem' seemed axiomatic through its counterfactual: a hypothetical organisational environment where cybersecurity decisions and strategy are not bottlenecked by epistemic considerations is one where traditional management and/or risk-based conceptual tools/models offer consistent and sufficient inferential support, leading to reasonably predictable and manageable outcomes. In contrast, the anecdotal and aggregate evidence concerning the role and attributes of cybersecurity efforts indicate a very different organisational dynamic than that postulated in this counterfactual. By following this line of enquiry, a picture of the relationship between objectives, mechanisms and epistemic structures which underpin this epistemic hostility is formed. Subsequently, a more general, theoretical problem is inferred: a gap between the emerging description/explanation of the context dynamics and the embedded assumptions of risk frameworks which are reiterations of approaches native to other traditional facets of risk. This diagnosis in itself has been problematic — given the plethora of risk frameworks, any reference to a monolithic approach is susceptible to exceptions and imprecision. Nonetheless, the effort to highlight and address the necessity for adequately representing the epistemic dynamics of organisational cybersecurity in prescriptive constructs/frameworks has been expressed through the 'context-construct gap' heuristic. By the end of the project's lifecycle, an explicit line of

philosophical, theoretical and empirical claims have been made to conceptualise the study's contributions. These are also an expression of researcher growth as an iterative process of trial and error, and express future research ambitions which could assess, validate, and supplement this lens of analysis.

.

7. References

Akerlof, G.A. (1970) 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism'. The Quarterly Journal of Economics 84 (3), 488

Allen, C.R., Angeler, D.G., Garmestani, A.S., Gunderson, L.H., and Holling, C.S. (2014) 'Panarchy: Theory and Application'. Ecosystems 17 (4), 578–589

Allen, P. and Boulton, J. (2011) 'Complexity and Limits to Knowledge: The Importance of Uncertainty' in The SAGE Handbook of Complexity and Management. Ed. by Allen, P., Maguire, S. and McKelvey, B. London: SAGE Publications, 164-181

Allen, P.M., Strathern, M., and Baldwin, J.S. (2007) 'Complexity and the Limits to Learning'. Journal of Evolutionary Economics 17 (4), 401–431

Anderson, R. and Moore, T. (2006) 'The Economics of Information Security.'. Science 314 (5799), 610–613

Association of British Insurers (2016) *ABI calls for database to help UK take lead in the global cyber insurance market* [online] available from <https://www.abi.org.uk/news/news-articles/2016/05/abi-calls-for-database-to-help-uk-take-lead-in-the-global-cyber-insurance-market/> [27 July 2018]

Attrition.org (2014) *Absolute Sownage: A concise history of recent Sony Hacks* [online] available from <http://attrition.org/security/rant/sony_aka_sownage.html> [26 July 2018]

Aven, T. (2012) 'The Risk Concept—Historical and Recent Development Trends'. ESREL 2007, the 18th European Safety and Reliability Conference 99 (C), 33–44

Aven, T. (2013) 'Practical Implications of the New Risk Perspectives'. ESREL 2007, the 18th European Safety and Reliability Conference 115 (C), 136–145

Aven, T. (2017) 'The Flaws of the ISO/IEC 31000 Conceptualisation of Risk'. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 231 (5), 467–468

Aven, T. and Zio, E. (2011) 'Some Considerations on the Treatment of Uncertainties in Risk Assessment for Practical Decision Making'. Reliability Engineering & System Safety 96 (1), 64–74

Baracaldo, N. and Joshi, J. (2013) 'An Adaptive Risk Management and Access Control

Framework to Mitigate Insider Threats'. Computers & Security 39 (PB), 237–254

Barford, P., Dacier, M., Dietterich, T.G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C., and Yen, J. (2009) 'Cyber SA: Situational Awareness for Cyber Defense'. in Cyber Situational Awareness. Advances in Information Security. vol. 46. vol. Boston, MA: Springer US, 3–13

Bauer, J.M. and van Eeten, M.J.G. (2009) 'Cybersecurity Stakeholder Incentives, Externalities, and Policy Options'. Telecommunications Policy 33 (10-11), 706–719

Beaudrie, C.E.H., Kandlikar, M., and Ramachandran, G. (2011) 'Using Expert Judgment for Risk Assessment'. in Assessing Nanoparticle Risks to Human Health. Elsevier, 109–138

Bechara, A. and Damasio, A.R. (2005) 'The Somatic Marker Hypothesis: a Neural Theory of Economic Decision'. Games and Economic Behavior 52 (2), 336–372

Beinhocker, E. D. (2007) 'The Origin of Wealth: Evolution, Complexity and the Radical Remaking of Economics'. London:Random House

Benbya, H. and McKelvey, B. (2006a) 'Toward a Complexity Theory of Information Systems Development'. Information Technology & People 19 (1), 12–34

Benbya, H. and McKelvey, B. (2006b) 'Using Coevolutionary and Complexity Theories to Improve IS Alignment: a Multi-Level Approach'. Journal of Information Technology 21 (4), 284–298

Berman, J. (2013) 'Utility of a Conceptual Framework Within Doctoral Study: a Researcher's Reflections'. Issues in Educational Research 23 (1), 1

Bhaskar, R. (2008) A Realist Theory of Science. Oxon:Routledge

Billings, M. (2016) *The Daily Startup: Increased Spending in Cybersecurity Drives Funding Surge* [online] available from <https://blogs.wsj.com/venturecapital/2016/02/17/the-daily-startup-increased-spending-in-cybersecurity-drives-funding-surge/> [26 July 2017]

Bingham, C.B. and Eisenhardt, K.M. (2011) 'Rational Heuristics: the "Simple Rules" That Strategists Learn From Process Experience'. Strategic Management Journal 32 (13), 1437–1464

Bjerga, T. and Aven, T. (2015) 'Adaptive Risk Management Using New Risk Perspectives – an Example From the Oil and Gas Industry'. Reliability Engineering & System Safety 134, 75–82

Bond, A., Morrison-Saunders, A., Gunn, J.A.E., Pope, J., and Retief, F. (2015) 'Managing

Uncertainty, Ambiguity and Ignorance in Impact Assessment by Embedding Evolutionary Resilience, Participatory Modelling and Adaptive Management'. Journal of Environmental Management 151 (C), 97–104

Bonifati, G. (2013) 'Exaptation and Emerging Degeneracy in Innovation Processes'. Economics of Innovation and New Technology 22 (1), 1–21

Breach Level Index (2018) *Data Breach Statistics* [online] available from <https://breachlevelindex.com> [27 July 2018]

Brighton, H. and Gigerenzer, G. (2015) 'The Bias Bias'. Journal of Business Research 68 (8), 1772–1784

Brinkmann, S. (2013) *Qualitative Interviewing.* Oxford:Oxford University Press

Broadhead, S. (2018) 'The Contemporary Cybercrime Ecosystem: a Multi-Disciplinary Overview of the State of Affairs and Developments'. Computer Law & Security Review 34 (6), 1180–1196

Bughin, J., Chui, M., and Manyika, J. (2015) *An executive's guide to the Internet of Things*[online] available from <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/an-executives-guide-to-the-internet-of-things> [29 July 2018)

Casey, E. (2004) 'Reporting Security Breaches – a Risk to Be Avoided or Responsibility to Be Embraced?'. Digital Investigation 1 (3), 159–161

Cave, J., van Oranje-Nassau, C., Schindler, H.R., Shehabi, A., Brutscher, P.-B., and Robinson, N. (2009) *Trends in Connectivity Technologies and Their Socioeconomic Impacts.* Cambridge: RAND Europe

Chmielewski, D. (2015) *Lessons of the Sony Hack: 'Anybody's Vulnerable"* [online] available from <http://recode.net/2015/02/28/lessons-of-the-sony-hack-anybodys-vulnerable-video/> [26 July 2018]

Clarke, L. (1988) 'Politics and Bias in Risk Assessment'. The Social Science Journal 25 (2), 155–165

Clinton, B (1998) *Presidential Decision Directive/NSC 63* [online] available from <https://fas.org/irp/offdocs/pdd/pdd-63.htm> [28 July 2018]

Covello, V.T. and Mumpower, J. (1985) 'Risk Analysis and Risk Management: an Historical Perspective'. Risk Analysis 5 (2), 103–120

Cox, L.A.T., Jr. (2012) 'Confronting Deep Uncertainties in Risk Analysis'. Risk Analysis 32

(10), 1607–1629

Daitch, H. (2017) *2017 Data Breaches - The Worst So Far* [online] available from <https://www.identityforce.com/blog/2017-data-breaches> [27 July 2018]

Dake, K. (1992) 'Myths of Nature: Culture and the Social Construction of Risk'. Journal of Social Issues 48 (4), 21–37

Dew, N. and Sarasvathy, S.D. (2016) 'Exaptation and Niche Construction: Behavioral Insights for an Evolutionary Theory'. Industrial and Corporate Change 25 (1), 167–179

Dickson, J. B. (2015) *We Need a New Word For Cyber* [online] available from <https://www.darkreading.com/attacks-breaches/we-need-a-new-word-for-cyber/a/d-id/1323278> [28 July 2018]

Diefenbach, T. (2009) 'Are Case Studies More Than Sophisticated Storytelling?: Methodological Problems of Qualitative Empirical Research Mainly Based on Semi-Structured Interviews'. Quality & Quantity 43 (6), 875–894

Easton, G. (2010) 'Critical Realism in Case Study Research'. Industrial Marketing Management 39 (1), 118–128

Eisenhardt, K.M. and Martin, J.A. (2000) 'Dynamic Capabilities: What Are They?'. Strategic Management Journal 21 (10-11), 1105–1121

Endsley, M.R. (1995) 'Toward a Theory of Situation Awareness in Dynamic Systems'. Human Factors: The Journal of the Human Factors and Ergonomics Society 37 (1), 32–64

ENISA (2019) *National Cybersecurity Strategies* [online] available from < https://www.enisa.europa.eu/topics/national-cyber-security-strategies> [29 January 2019]

European Commission (2013) *EU Cybersecurity plan to protect open internet and online freedom and opportunity – Cyber Security strategy and Proposal for a Directive* [online] available from <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security> [24 May 2018]

Faucher, J.B.P.L., Everett, A.M., and Lawson, R. (2008) 'Reconstituting Knowledge Management'. Journal of Knowledge Management 12 (3), 3–16

Ferdinado, L. (2015) Dempsey: Cyber Vulnerabilities Threaten National Security [online] available from <https://www.defense.gov/News/Article/Article/603952/> [26 July 2018]

FireEye (2018) *M-Trends 2018* [online] available from <https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf>

Firestone, J. M. and McElroy, M. W. (2003) *Key Issues in The New Knowledge Management*. Boston:Elsevier

Flyvbjerg, B. (2006) 'Five Misunderstandings About Case-Study Research'. Qualitative Inquiry 12 (2), 219–245

Folke, C. (2006) 'Resilience: the Emergence of a Perspective for Social–Ecological Systems Analyses'. Global Environmental Change 16 (3), 253–267

Franke, U. and Brynielsson, J. (2014) 'Cyber Situational Awareness - a Systematic Review of the Literature'. Computers & Security 46 (C), 18–31

Gal-Or, E. and Ghose, A. (2005) 'The Economic Incentives for Sharing Security Information'. Information Systems Research 16 (2), 186–208

GAO (2018) *DATA PROTECTION: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach* [online] available from < https://www.gao.gov/products/GAO-18-559> [29 January 2019]

Garud, R., Gehman, J., and Giuliani, A.P. (2016) 'Technological Exaptation: a Narrative Approach'. Industrial and Corporate Change 25 (1), 149–166

Gemalto (2016) *2015 Data Breach Statistics: The Good, the Bad, and the Ugly* [online] available from <https://blog.gemalto.com/security/2016/03/03/2015-data-breaches-by-the-numbers/> [27 July 2018]

Gershenson, C. (2013) 'The Implications of Interactions for Science and Philosophy'. Foundations of Science 18 (4), 781–790

Gigerenzer, G. (1996) 'On Narrow Norms and Vague Heuristics: a Reply to Kahneman and Tversky.'. Psychological Review 103 (3), 592–596

Gigerenzer, G. and Brighton, H. (2009) 'Homo Heuristicus: Why Biased Minds Make Better Inferences'. Topics in Cognitive Science 1 (1), 107–143

Gilovich T., Vallone, R. and Tversky, A. (2002) 'The Hot Hand in Basketball: On the Misperception of Random Sequences'. In Heuristics and Biases. ed. by Gilovich, T., Griffin, D. and Kahneman, D. Cambridge: Cambridge University Press

Goldberg, R. (2016) *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities [*online] available from

<https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities> [26 July 2018]

Goldstein, J. (2011) 'Emergence in Complex Systems' in The SAGE Handbook of Complexity and Management. Ed. by Allen, P., Maguire, S. and McKelvey, B. London: SAGE Publications, 65-78

Gould, S.J. and Vrba, E.S. (1982) 'Exaptation—a Missing Term in the Science of Form'. Paleobiology 8 (1)

GOV.UK (2018) *Cyber Essential Scheme: Overview* [online] available from <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview> [26 July 2018]

GOV.UK (2018) *Cyber Security Breaches Survey 2018* [online] available from <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018> [26 July 2018]

Gowdy, J.M. (1992) 'Higher Selection Processes in Evolutionary Economic Change'. Journal of Evolutionary Economics 2 (1), 1–16

GPO (2002) *Cyber Security Enhancement Act of 2002* [online] available from <https://www.gpo.gov/fdsys/granule/USCODE-2010-title6/USCODE-2010-title6-chap1-subchapII-partC-sec145> [28 July 2018]

Grant Thornton (2016) *Adapting to Change: The Financial Health of the Higher Education Sector in the UK 2016* [online] available from <https://www.grantthornton.co.uk/globalassets/1.-member-firms/united-kingdom/pdf/publication/2016/financial-health-of-the-higher-education-sector-2016.pdf> [28 July 2018]

Greenberg, A. (2012) *Cybersecurity Bill's Backers Cite Antivirus Firms' Bogus Cybercrime Stats* [online] available from <http://www.forbes.com/sites/andygreenberg/2012/08/02/cybersecurity-bills-backers-cite-antivirus-firms-bogus-cybercrime-stats/> [24 May 2018]

Greenberg, A. (2016) *The Jeep Hackers Are Back To Prove Car Hacking Can Get Much Worse* [online] available from <https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/> [26 July 2018]

Haimes, Y.Y. (2011) 'On the Complex Quantification of Risk: Systems-Based Perspective

on Terrorism'. Risk Analysis 31 (8), 1175–1186

Haimes, Y.Y. (2012) 'Systems-Based Guiding Principles for Risk Modeling, Planning, Assessment, Management, and Communication'. Risk Analysis 32 (9), 1451–1467

Haldane, A.G. (2009) Why Banks Failed the Stress Test. 1–23

Harris, L.C. and Ogbonna, E. (2002) 'The Unintended Consequences of Culture Interventions: a Study of Unexpected Outcomes'. British Journal of Management 13 (1), 31–49

Henrickson, L. and McKelvey, B. (2002) 'Foundations of "New" Social Science: Institutional Legitimacy From Philosophy, Complexity Science, Postmodernism, and Agent-Based Modeling'. Proceedings of the National Academy of Sciences 99 (suppl 3), 7288–7295

HESA (2017) *Higher Education Statistics for the UK 2015/16* [online] available from <https://www.hesa.ac.uk/data-and-analysis/publications/higher-education-2015-16> [28 July 2018]

Heuer, R.J.J. (1999) Psychology of Intelligence Analysis. Center for the Study of Intelligence

Hogan Lovells (2016) *The UK's Cybersecurity Regulatory Landscape: An Overview* [online] available from <http://www.hldataprotection.com/2016/12/articles/international-eu-privacy/the-uks-cybersecurity-regulatory-landscape-an-overview/>

Holling, C.S. (2001) 'Understanding the Complexity of Economic, Ecological, and Social Systems'. Ecosystems 4 (5), 390–405

ICO (2017) *Guide to the General Data Protection Regulation (GDPR)* [online] available from <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/> [28 July 2018]

ISO/IEC (2013) *Information technology - Security techniques - Information security management systems - Requirements*. ISO/IEC 27001:2013. Geneva: ISO

ISO/IEC (2018) *Information technology – Security techniques – Information security risk management.* ISO/IEC 27005: 2018. Geneva: ISO

Jabareen, Y. (2009) 'Building a Conceptual Framework: Philosophy, Definitions, and Procedure'. International Journal of Qualitative Methods 8 (4), 49–62

JISC (2017) *Cybersecurity Posture Survey 2017 Research Findings* [online] available from

<https://community.JISC.ac.uk/system/files/288/Cybersecurity%20Posture%20Survey%202017%20Research%20Findings.pdf> [28 July 2018]

Juarrero, A. (2011) 'Causality and Explanation' in The SAGE Handbook of Complexity and Management. Ed. by Allen, P., Maguire, S. and McKelvey, B. London: SAGE Publications, 155-163

Julisch, K. (2013) 'Understanding and Overcoming Cyber Security Anti-Patterns'. Computer Networks 57 (10), 2206–2211

Kahneman, D. and Frederick, S. (2002) 'Representativeness Revisited: Attribute Substitution in Intuitive Judgment'. In Heuristics and Biases. ed. by Gilovich, T., Griffin, D. and Kahneman, D. Cambridge: Cambridge University Press

Klarh, R., Shah, J. N., Sheriffs, P., Rossington, R., Pestell, G., Button, M. and Wang, V. (2017) *Cyber security breaches survey 2017* [online] available from <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017> [28 July 2018]

Klein, H.K. (2004) 'Seeking the New and the Critical in Critical Realism: Déjà Vu?'. Information and Organization 14 (2), 123–144

Knight, S. and Cross, D. (2012) 'Using Contextual Constructs Model to Frame Doctoral Research Methodology'. International Journal of Doctoral Studies 7, 039 – 062

Koehler, J.J. (1996) 'The Base Rate Fallacy Reconsidered: Descriptive, Normative, and Methodological Challenges'. Behavioral and Brain Sciences 19 (1), 1–17

Kowal, S. and O'Connell, D. (2014) 'Transcription as a Crucial Step of Data Analysis' in The SAGE Handbook of Qualitative Data Analysis. Ed. by Flick, U. London: SAGE Publications, 64-78

Kraemer-Mbula, E., Tang, P., and Rush, H. (2013) 'The Cybercrime Ecosystem: Online Innovation in the Shadows?'. Future-Oriented Technology Analysis 80 (3), 541–555

Kraemer, S. and Carayon, P. (2007) 'Human Errors and Violations in Computer and Information Security: the Viewpoint of Network Administrators and Security Specialists'. Applied Ergonomics 38 (2), 143–154

Kraemer, S., Carayon, P., and Clem, J. (2009) 'Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities'. Computers & Security 28 (7), 509–520

Krugman, P. (1998) ‘Rationales for Rationality’. in Rationality in Economics: Alternative Perspectives. ed. by Dennis, K. Rationality in Economics: Alternative Perspectives. Dordrecht: Springer Netherlands, 111–122

Kuehl, D.T. (2009) ‘From Cyberspace to Cyberpower: Defining the Problem ’. in Cyberpower and National Security. 1st edn. ed. by Kramer, F.D., Starr, S.H., and Wentz, L. Virginia, 24–43

Laland, K.N., Odling-Smee, J., and Feldman, M.W. (2000) ‘Niche Construction, Biological Evolution, and Cultural Change’. Behavioral and Brain Sciences 23 (1), 131–146

Lansing, J.S. (2003) ‘Complex Adaptive Systems’. Annual Review of Anthropology 32 (1), 183–204

Larson, G., Stephens, P.A., Tehrani, J.J., and Layton, R.H. (2013) ‘Exapting Exaptation’. Trends in Ecology & Evolution 28 (9), 497–498

Levy, D. (1994) ‘Chaos Theory and Strategy: Theory, Application, and Managerial Implications’. Strategic Management Journal 15, 167–178

Linkov, I., Satterstrom, F.K., Kiker, G., Batchelor, C., Bridges, T., and Ferguson, E. (2006) ‘From Comparative Risk Assessment to Multi-Criteria Decision Analysis and Adaptive Management: Recent Developments and Applications’. Environment International 32 (8), 1072–1093

Maguire, S. (2011) ‘Constructing and Appreciating Complexity’ in The SAGE Handbook of Complexity and Management. Ed. by Allen, P., Maguire, S. and McKelvey, B. London: SAGE Publications, 79-92

Mandiant (2016) *M-Trends 2016* [online] available from <https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-2016-mtrends.html> [27 July 2018]

Manson, S.M. (2001) ‘Simplifying Complexity: a Review of Complexity Theory’. Geoforum 32 (3), 405–414

March, J.G. (1978) ‘Bounded Rationality, Ambiguity, and the Engineering of Choice’. The Bell Journal of Economics 9 (2), 587

March, J.G. (2006) ‘Rationality, Foolishness, and Adaptive Intelligence’. Strategic Management Journal 27 (3), 201–214

Mark, J.T., Marion, B.B., and Hoffman, D.D. (2010) ‘Natural Selection and Veridical

Perceptions'. Journal of Theoretical Biology 266 (4), 504–515

Mason, R.B. (2007) 'The External Environment's Effect on Management and Strategy'. Management Decision 45 (1), 10–28

Matsumoto, D. (2007) 'Culture, Context, and Behavior'. Journal of Personality 75 (6), 1285–1320

Maxwell, J. A. and Chimel, M. (2014) 'Notes Towards a Theory of Qualitative Data Analysis' in The SAGE Handbook of Qualitative Data Analysis. Ed. by Flick, U. London: SAGE Publications, 21-34

McAfee (2014) *Net Losses: Estimating The Global Cost of Cybercrime* [online] available from <http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/McAfee%20and%20CSIS%20-%20Econ%20Cybercrime.pdf> [26 July 2018]

McAfee (2018) *The Economic Impact of Cybercrime - No Slowing Down* [online] available from <https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf>[26 July 2018]

McElroy, M. W. (2000) 'Integrating Complexity Theory, Knowledge Management and Organizational Learning'. Journal of Knowledge Management 4 (3), 195–203

McElroy, M. W. (2003) *The New Knowledge Management: Complexity, Learning, and Sustainable Innovation*. Boston:Elsevier

McFall, J.P. (2015) 'Rational, Normative, Descriptive, Prescriptive, or Choice Behavior? the Search for Integrative Metatheory of Decision Making.'. Behavioral Development Bulletin 20 (1), 45–59

McKelvey, B. (2001) 'What Is Complexity Science?'. Emergence 3 (1), 137–157

Merali, Y. and Allen, P. (2011) 'Complexity and Systems Thinking' in The SAGE Handbook of Complexity and Management. Ed. by Allen, P., Maguire, S. and McKelvey, B. London: SAGE Publications, 31-52

Mercier, H. and Sperber, D. (2011) 'Why Do Humans Reason? Arguments for an Argumentative Theory'. Behavioral and Brain Sciences 34 (02), 57–74

Miles, M. B., Huberman, M. A. and Saladana, J. (2014) *Qualitative Data Analysis: A Methods Sourcebook*. London: SAGE Publications

Miller, J.H. and Page, S.E. (2007) Complexity in Social Worlds. Princeton: Princeton

University Press

Moore, T. (2010) 'The Economics of Cybersecurity: Principles and Policy Options'. International Journal of Critical Infrastructure Protection 3 (3-4), 103–117

Mousavi, S. and Gigerenzer, G. (2014) 'Risk, Uncertainty, and Heuristics'. Journal of Business Research 67 (8), 1671–1678

NCA (2016) *Cyber Crime Assessment 2016: Need for a stronger law enforcement and business partnership to fight cyber crime* [online] available from <http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file> [29 July 2018]

NCA (2018) *National Strategic Assessment of Serious and Organised Crime* [online] available from <http://www.nationalcrimeagency.gov.uk/publications/905-national-strategic-assessment-for-soc-2018/file> [27 July 2018]

Nielsen, S.C. (2012) 'Pursuing Security in Cyberspace: Strategic and Organizational Challenges'. Orbis 56 (3), 336–356

NIST (2011) *Managing Information Security Risk*. NIST SP800-39:2011. Gaithersburg:NIST

NIST (2018) *Framework for Improving Critical Infrastructure Cybersecurity* [online] available from < https://www.nist.gov/cyberframework/framework> [26 January 2019]

Obama, B. (2009) Remarks by the President on Securing Our Nation's Cyber Infrastructure [online] available from <https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure> [05 July 2018]

Osbourne, C. (2015) *Most companies take over six months to detect data breaches [online] available form* <http://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/> [24 May 2018]

Patton, M.Q. (1990) 'Qualitative Evaluation and Research Methods'. in Designing Qualitative Studies. SAGE Publications, Incorporated, 168–186

Peters, K., Maruster, L., and Jorna, R.J. (2010) 'Knowledge Claim Evaluation: a Fundamental Issue for Knowledge Management'. Journal of Knowledge Management 14 (2), 243–257

Pfleeger, S.L. and Caputo, D.D. (2012) 'Leveraging Behavioral Science to Mitigate Cyber Security Risk'. Computers & Security 31 (4), 597–611

Phister, P.W. (2010) ‘Cyberspace: the Ultimate Complex Adaptive System’. The International C2 Journal 4, 1–30

Popper, K. (1978) ‘Three Worlds’. in The Tanner Lecture on Human Values. The University of Michigan, 143–167

Prince, M. (2016) *Empty DDoS Threats: Meet the Armada Collective* [online] available from <https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective/>

PWC (2015) *2015 Information Security Breaches Survey* [online] available from <https://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-digital.pdf> [26 July 2018]

PWC (2016) Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey [online] available from <http://www.cyberriskinsuranceforum.com/sites/default/files/pictures/pwc-global-state-of-information-security-survey-20%20%5Bfull%5D.pdf> [27 July 2017

Reece, R.P. and Stahl, B.C. (2015) ‘The Professionalisation of Information Security: Perspectives of UK Practitioners’. Computers & Security 48 (C), 182–195

Reichertz, J. (2014) 'Induction, Deduction, Abduction' in The SAGE Handbook of Qualitative Data Analysis. Ed. by Flick, U. London: SAGE Publications, 123-135

Rickles, D., Hawe, P., and Shiell, A. (2007) ‘A Simple Guide to Chaos and Complexity’. Journal of Epidemiology & Community Health 61 (11), 933–937

Rid, T. and Buchanan, B. (2014) ‘Attributing Cyber Attacks’. Journal of Strategic Studies 38 (1-2), 4–37

Romanosky, S. (2016) ‘Examining the Costs and Causes of Cyber Incidents’. Journal of Cybersecurity 01–15

Roulston, K. (2014) 'Analysing Interviews' in The SAGE Handbook of Qualitative Data Analysis. Ed. by Flick, U. London: SAGE Publications, 297-312

Sabau, G.L. (2010) ‘Know, Live and Let Live: Towards a Redefinition of the Knowledge-Based Economy — Sustainable Development Nexus’. Ecological Economics 69 (6), 1193–1201

Saunders, B., Kitzinger, J., and Kitzinger, C. (2014) ‘Anonymising Interview Data: Challenges and Compromise in Practice’. Qualitative Research 15 (5), 616–632

Schneier, B. (2014) *Lessons from the Sony Hack* [online] available from

<https://www.schneier.com/blog/archives/2014/12/lessons_from_th_4.html> [26 July 2018]

Schwarz, N. and Vaughn, L. A. (2002) 'The Availability Heuristic Revisited: Ease of Recall and Content of Recall as Distinct Sources of Information'. In Heuristics and Biases. ed. by Gilovich, T., Griffin, D. and Kahneman, D. Cambridge: Cambridge University Press

Sharma, S. and Dhillon, G. (2009) 'IS Risk Analysis: a Chaos Theoretic Perspective'. Issues in Information Systems 10 (2), 552–560

Shedden, P., Scheepers, R., Smith, W., and Ahmad, A. (2011) 'Incorporating a Knowledge Perspective Into Security Risk Assessments'. VINE 41 (2), 152–166

Simon, H.A. (1962) 'The Architecture of Complexity'. Proceedings of the American Philosophical Society 106 (6), 467–482

Singelis, T.M. and Brown, W.J. (1995) 'Culture, Self, and Collectivist Communication Linking Culture to Individual Behavior'. Human Communication Research 21 (3), 354–389

Slaughter and May (2016) *Cyber Security: Corporate Insights for Companies and Their Directors* [online] available from <https://www.slaughterandmay.com/media/2536333/cyber-security-corporate-insights-for-companies-and-their-directors.pdf> [27 July 2018]

Sloman, S. A. (2002) 'Two Systems of Reasoning'. In Heuristics and Biases. ed. by Gilovich, T., Griffin, D. and Kahneman, D. Cambridge: Cambridge University Press

Sloman, S.A., Fernbach, P.M., and Ewing, S. (2012) 'A Causal Model of Intentionality Judgment'. Mind & Language 27 (2), 154–180

Slovic, P., Peters, E., Finucane, M.L., and MacGregor, D.G. (2005) 'Affect, Risk, and Decision Making.'. Health Psychology 24 (4, Suppl), S35–S40

Smith, M.E. (2003) 'Changing an Organisation's Culture: Correlates of Success and Failure'. Leadership & Organization Development Journal 24 (5), 249–261

Snowden, D. (2002) 'Complex Acts of Knowing: Paradox and Descriptive Self-Awareness'. Journal of Knowledge Management 6 (2), 100–111

Sommestad, T., Ekstedt, M., and Johnson, P. (2010) 'A Probabilistic Relational Model for Security Risk Analysis'. Computers & Security 29 (6), 659–679

Hoo, K. J. (2000) *How Much is Enough? A Risk-Management Approach to Computer Security*. PhD thesis. Stanford:Stanford University

Sperber, D. and Mercier, H. (2012) Reasoning as a Social Competence. ed. by Landemore, H. and Elster, J. Principles and Mechanisms. Cambridge: Cambridge University Press

Sunstein, C.R. (1996) 'Social Norms and Social Roles'. Columbia law review 96 (4), 903

Tadda, G.P. and Salerno, J.S. (2010) 'Overview of Cyber Situation Awareness'. in Cyber Situational Awareness: Issues and Research. ed. by Jajodia, S., Liu, P., Swarup, V., and Wang, C. Cyber Situational Awareness: Issues and Research. Boston, MA: Springer US, 15–35

Tansey, J. and O'Riordan, T. (1999) 'Cultural Theory and Risk: a Review'. Health, Risk & Society 1 (1), 71–90

Teece, D.J., Pisano, G., and Shuen, A. (1997) 'Dynamic Capabilities and Strategic Management'. Strategic Management Journal 18 (7), 509–533

Thaler, R.H. (2000) 'From Homo Economicus to Homo Sapiens'. Journal of Economic Perspectives 14 (1), 133–141

Thomas, K., Huang, D.Y., Wang, D.Y., Bursztein, E., Grier, C., Holt, T., Kruegel, C., McCoy, D., Savage, S., and Vigna, G. (2015) 'Framing Dependencies Introduced by Underground Commoditization.'. WEIS

Thomas, K., Yuxing, D., David, H., Elie, W., and Grier, B.C. (2015) 'Framing Dependencies Introduced by Underground Commoditization'. In Proceedings (online) of the Workshop on Economics of Information Security (WEIS)

Thomson, K.-L., Solms, von, R., and Louw, L. (2006) 'Cultivating an Organizational Information Security Culture'. Computer Fraud & Security 2006 (10), 7–11

Tsang, E.W.K. (2014) 'Case Studies and Generalization in Information Systems Research: a Critical Realist Perspective'. Journal of Strategic Information Systems 23 (2), 174–186

Tversky, A. and Kahneman, D. (1974) 'Judgment Under Uncertainty: Heuristics and Biases'. Science 185 (4157), 1124–1131

Tversky, A. and Kahneman, D. (2002) 'Extensional versus Intuitive Reasoning: The Conjunction Fallacy in Probability Judgement'. In Heuristics and Biases. ed. by Gilovich, T., Griffin, D. and Kahneman, D. Cambridge: Cambridge University Press

UK Government (2009) *Cyber Security Strategy of the United Kingdom* [online] available from

<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf> [24 May 2018]

UK Government (2011) *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* [online] available form <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> [24 May 2018]

UK Government (2016) *National Cyber Security Strategy 2016 to 2021* [online] available from <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf> [29 January 2019]

UK Parliament (2015) *Cyber crime and cyber security: Key issues for the 2015 Parliament* [online] available from <https://www.parliament.uk/business/publications/research/key-issues-parliament-2015/defence-and-security/cyber-security/> [26 August 2018]

Ulieru, M. and Worthington, P. (2006) 'Adaptive Risk Management System (ARMS) for critical infrastructure protection'. Integrated Computer-Aided Engineering, 13 (1), 63-80

US Congress (2015) *S.754 - To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes* [online] available from <https://www.congress.gov/bill/114th-congress/senate-bill/754> [26 July 2018]

Vmware (2016) *University Challenge: Cyber Attacks in Higher Education* [online] available from <https://www.nextgensecurityforeducation.com/wp-content/uploads/VMWare-UK-University-Challenge-Cyber-Security.pdf> [28 July 2018]

Walker, B., Gunderson, L., Kinzig, A., and Folke, C. (2006) 'A Handful of Heuristics and Some Propositions for Understanding Resilience in Social-Ecological Systems'. Ecology and Society 11 (1), art13

White House (2010) *Cyberspace Policy Review* [online] available from <https://obamawhitehouse.archives.gov/cyberreview/documents/> [28 July 2018]

White House (2011) *Cybersecurity Legislative Proposal* [online] available from <https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf> 28 July 2018

White House (2013) *Executive Order – Improving Critical Infrastructure Cybersecurity*

[online] available from <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity> [5 July 2015]

White House (2015) *Executive Order – Promoting Private Sector Cybersecurity Information Sharing* [online] available from <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari> [26 July 2018]

White House (2018) National Cyber Strategy of the United States of America [online] available from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [29 January 2019]

White, G. B. (2017) *A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable* [online] available from <https://www.theatlantic.com/business/archive/2017/09/equifax-cybersecurity-breach/539178/> [27 July 2018]

Willig, C. (2014) 'Interpretation and Analysis' in The SAGE Handbook of Qualitative Data Analysis. Ed. by Flick, U. London: SAGE Publications, 136-150

Winter, T. and Brunker, M. (2017) *Thieves tweaked 'off-the-shelf' malware for Target data heist, security firm says* [online] available from <http://investigations.nbcnews.com/_news/2014/01/17/22341717-thieves-tweaked-off-the-shelf-malware-for-target-data-heist-security-firm-says> [26 July 2018]

Wintle, B.A. and Lindenmayer, D.B. (2008) 'Adaptive Risk Management for Certifiably Sustainable Forestry'. Forest Ecology and Management 256 (6), 1311–1319

Wynn, D.E., Jr and Williams, C.K. (2012) 'Principles for Conducting Critical Realist Case Study Research in Information Systems.'. MIS quarterly 36, 787–810

Yin, R. (2003) *Case study research: design and methods*. Thousand Oaks: SAGE Publications

Zachariadis, M., Scott, S., and Barrett, M. (2013) 'Methodological Implications of Critical Realism for Mixed-Methods Research'. MIS quarterly 37 (3), 855–879

Zachmann, K. (2014) 'Risk in Historical Perspective: Concepts, Contexts, and Conjunctions'. in Risk - a Multidisciplinary Introduction. ed. by Klüppelberg, C., Straub, D., and Welpe, I.M. Cham: Springer International Publishing, 3–35

Ziv, A. (1993) ‘Information Sharing in Oligopoly: the Truth-Telling Problem’. The RAND Journal of Economics 24 (3), 455

8. Appendices

Appendix 1: Informed Consent Form

Conceptualising Adaptive Cyber Risk Management:

Project Summary: Organisations face unprecedented pressures to defend their assets base, while leveraging technology in order to maximise and sustain value generation. The effective formulation of Cybersecurity Management strategy, which generally relies on risk frameworks, is predicated on an overarching knowledge problem: how can the net benefits of cyber presence be maximised without exposing the organisation to unforeseen existential threats? The current project aims to conceptualise a Risk based framework addressing the Knowledge-Uncertainty dimension of cybersecurity management through a meta-analysis of current approaches, an empirical investigation of the problem in a complex organisational environment, and the development of an alternative chain of inference regarding operational assumptions to account for non-linear dynamics, bound rationality, and meta-disciplinary novel risk perspectives. Following the literature review, six topics have been identified and used to guide data collection: Change/Dynamics, Rationality, Knowledge, Uncertainty, Risk and Adaptation. The empirical theory building process is inductive, following an embedded case study which aims to capture a hierarchy of actor perspectives in relation to the proposed topics.

	Please initial
1. I confirm that I have read and understood the participant information sheet (insert version number) for the above study and have had the opportunity to ask questions	☐
2. I understand that my participation is voluntary and that I am free to withdraw at any time without giving a reason	☐
3. I understand that all the information I provide will be treated in confidence	☐
4. I understand that I also have the right to change my mind about participating in the study for a short period after the study has concluded (able to withdraw by December 2017)	☐
5. I agree to be recorded and for anonymised quotes to be used as part of the research project	☐
6. I agree to take part in the research project	☐

Name of participant:

Signature of participant:

Date:

Appendix 2: Participant Information Sheet

Conceptualising Adaptive Cyber Risk Management

What is the purpose of the study?

The project is a PhD thesis which aims to explore how cyber resilience and effective cybersecurity decision making can be supported through Adaptive Cyber Risk Management. More specifically, the models proposed within the study are designed to optimise how organisations navigate the uncertainty and predictive limitations which shape cybersecurity as a knowledge problem.

Why have I been chosen?

You have been invited to contribute due to your role, experience and expertise with aspects of the research problem.

How do I take part?

Upon confirming your decision to participate in the study, you will be contacted to establish a favourable time and setting (i.e. e-mail, Skype, or face to face) for an interview. This interview will consist of a series of open questions, which have been formulated around six conceptual themes in relation to cybersecurity management: Change, Rationality, Knowledge, Uncertainty, Risk and Adaptation. Your views will be recorded and safely stored (using hardware encryption) while the data will be anonymised. The series of interviews will then be used to develop a study, which will supplement theory for the development of a conceptual framework for Adaptive Cyber Risk management.

Do I have to take part?

No. Participation is on a purely voluntary basis. Furthermore, you can withdraw from the study at any point prior to 1st December 2017.

What will happen to me if I take part?

Upon giving your explicit agreement to participate, you will be contacted via e-mail or telephone in order to establish a suitable date, time and place/platform (i.e. Skype, FaceTime, e-mail, or telephone) for the conversation/interview. Once the logistical details have been arranged, the interview can proceed, and is expected to last approximately 45 minutes.

What are the possible disadvantages and risks of taking part?

There are no foreseeable disadvantages or risks which could occur as a result of the participation Before collecting any notes or recordings, explicit consent will be sought, and all collected data will be kept confidentially, and encrypted (256 bit AES) prior to storage. Personal identification data will be anonymised. Furthermore, you are encouraged to skip any question which may lead to disclosing sensitive information, or makes you uncomfortable.

What are the possible advantages of taking part?

In addition to providing a valuable contribution based on your expertise, electronic copies of the final project can be delivered to you at request, upon its completion.

What if something goes wrong?

In the event of any anomaly, or discomfort, the interview can be temporarily or permanently interrupted, based on the nature of the circumstances and the desire of the participants.

Will my taking part in this study be kept confidential?

While general attributes such as the primary area of expertise/parameters of the role will be kept to contextualise the feedback, no uniquely identifying personal information (i.e. Name, Age, or Affiliated Institution) of the participants will be disclosed or used within the study.

What will happen to the results of the research study?

The data will be used for the purpose of informing a doctoral thesis and academic publication.

Contact for Further Information

[Redacted]

Contact for Complaints

[Redacted]

Appendix 3: Interview Topics and Questions

In order to obtain ethical approval and stakeholder feedback, the base set of questions aimed to be exhaustive and self-sufficient in terms of its direction/meaning. In practice, the interview narrative was adapted for each participant, based on their role and experience, as a way to support a conversational dynamic. Based on the early interviews, a colour coding framework was developed in order to be able to maintain structural consistency without relying on a set body of text. As a result, grey text covers question narrative and qualifiers, or low priority/efficacy questions; Black text highlights the full question body; Red text covers key words and questions, which can be identified at a glance in a conversation.

Group 1: Strategy & Decision-making

- *Rationale of enquiry* (Top-down view): How Cyber Risks are positioned in a wider decision-making context; How Risk Assessments are perceived and utilised to inform policy and action; How adaptation is pursued.

Theme	Questions
Change	• A unique attribute of cyberspace, and, implicitly cybersecurity (cyber risk), is the elimination of boundaries in space (geography) and time which would otherwise constrain possible interactions. As a result, organisations have to defend a highly dynamic asset base against an ever-changing set of cyber threats. Is this pace of change a concern for decision-making? Does it affect the implementation of existing decision support methods – i.e. risk management? • How do macro-governance/cyber policy initiatives impact the cybersecurity climate of (your) individual organisation(s)? How should they? • The issue of cyber resilience has been increasingly addressed as a priority for both organisational and national security. However, the number of organisations which have visibly collapsed due to a cyber incident is still limited. How do you perceive cyber resilience, in relation to organisational resilience? • Available figures – i.e. aggregate cost of cyber incidents to the economy, or average annual cost for organisations – indicate a sense of predictive consistency and linearity. Nonetheless, when looking at attribution and forensics at an incident level, it seems that, absent hindsight, defenders face a much less consistent reality. How predictable are cybersecurity phenomena? Is there a discrepancy between different levels (macro/micro)? • There are a number of conflicting views concerning the nature of cybersecurity assessments. For example, a mechanistic view entails a problem which can be deconstructed into its components without significantly diminishing the effectiveness of the analysis, whereas a holistic perspective would indicate that such a deconstruction would neglect essential features of the system as a whole. Which, in your view, is a more adequate approach? • Within your industry, to what extent do you perceive the cybersecurity phenomena faced by your institution as general, or context-specific?
Rationality	• Does intuition play a role in cybersecurity strategy formulation and decision making? Should it? Can intuitive contributions be distinguished and (retrospectively) evaluated? • The literature on the use of Heuristics/Rules-of-thumb in situations of deep uncertainty is divided, placing them as both potentially effective in situations of uncertainty, particularly within the context of strategy, as well as a source of potential bias. How do you view the use of Heuristics within Cybersecurity decision-making? • Are biases and perceptual limitations an explicit concern for decision making? (If yes: how are they mitigated against)? • Assumptions are a key part of modeling and mitigating uncertainty. In your view, how relevant is the externalisation of assumptions outside of the risk analysis/modeling stage? • How can cybersecurity risk outputs be best communicated, given their abstract nature, without altering their original meaning/implications?

Knowledge	• How relevant is cybersecurity knowledge for organisations within your industry? How can such knowledge be acquired? • How would you position sector-wide cybersecurity knowledge availability in relation to other aspects of organisational risk? • What are the key criteria one could use for validating such knowledge? • Can the strength of the knowledge used to generate various risk assessments be differentiated? Does such a differentiation play an explicit part of the decision-making process? • Knowledge sharing has been presented as a potential method of mitigating the uncertainty faced by organisations in relation to their cybersecurity. However, given the sensitive nature of the information that would need to be shared for this to be useful, the adoption of such measures is still not significant in many industries/regions. Is knowledge sharing feasible within your context? To what extent? (stakeholders, or wider industry)
Uncertainty	• When compared to other aspects of organisational decision-making, how would you classify the uncertainty faced within cybersecurity management? Why? • What approaches for uncertainty mitigation could prove to be effective within your industry? (i.e risk/resilience management) • In your view, how would you expect this uncertainty to evolve in the near/mid-term? Why?
Risk	• Risk frameworks are presented by industry research bodies as the dominant approach for driving Cybersecurity Management efforts. In spite of their popularity, they also have critics who question the utility of risk concepts in given the extent of the uncertainty faced by decision makers in Cybersecurity. How would you assess the utility of risk frameworks in your organisation's context, based on your role and experience? • What role do Risk frameworks play within the scope of the wider decision-making landscape? • Can an effective implementation of Risk be distinguished from less effective alternatives? How?
Adaptation	• To what extent do macro-environmental trends (i.e changes in threat patterns, or additional support through policy) affect the local 'reality' faced by your institution/industry? In what ways? • *What distinguishes, in your view, an effective Cybersecurity strategy?* • What potential sources/strategies of feedback inform the evaluation of strategic performance?

Group 1*: Decision Making and Sector Oversight

- *Rationale of enquiry* (Macro-view): How sector wide bodies perceive and engage with Cybersecurity phenomena; their role and the scope of their support; their experience with institutional stakeholders; the implications of this macro-perspective within for the Case.

Theme	Questions/Topics of Discussion
Change	• Role of [Oversight Bodies] in relation to sector CS; • Perception of CS in the sector– Change/Evolving; • In your experience, how is CS viewed by HE/FE institutions? Is it Homogenous? Is it Changing?
Rationality	• Communicating Risk: Given its abstract nature, how can Risk be communicated effectively? • Have you experienced bias in relation to CS as part of your role?*
Knowledge and Uncertainty	• What does CS Knowledge look like across institutions? • How can it be validated/evaluated (strength of knowledge)? • Level of Uncertainty faced by Decision makers;
Risk	• What is the prevalence of Risk Frameworks at a sector level? • What sets apart an effective implementation of Risk Management?
Adaptation	• What sets apart an effective CS Strategy? • What sources and strategies of feedback are in the relationship between [Oversight Body] and individual institutions?

Group 2: Risk & Analysis

- *Rationale of enquiry*: How Cybersecurity decision-making is supported; How Risk outputs are conceptualized; How uncertainty is analysed and managed.

Theme	Questions
Change	• At an interdisciplinary level, the popularity of 'Risk'-based constructs has gained significant momentum throughout the last decades. However, this has produced a variety of approaches to risk, which depend on its disciplinary/industrial context. Do you view Cybersecurity as a distinct application-setting for Risk thinking? In what ways? • What are the most defining trends which, in your view, shape current Cybersecurity practices. How have these changed throughout your experience with Risk? • Factors such as the interdependencies, high pace and non-locality which characterise the interaction between actors in Cyberspace indicate highly complex potential interaction patterns/scenarios. How can Risk practitioners mitigate against unmanageable complexity? • Converting a continuous phenomenon into discrete sections can be important for structured decision making and modeling. However, it can also lead to the misidentification of patterns and regularities. Can the variable pace of change/system dynamics be accounted for in Cyber Risk assessments? How? • One of the defining features of Cyber Risk is the disproportionality between cause and effect. Seemingly small actions and vulnerabilities can lead to very significant effects. Is this disproportionality apparent in your experience? How does it affect the Risk modeling process?
Rationality	• What is your perception concerning the role of intuition in the risk assessment process? Can it be explicitly used as an input? • In your experience, is the chain of inference (sequence of logical steps and assumptions used to construct a risk assessment) made explicit? If yes, is it used to inform decision making by actors outside of the process? • In his analysis of the 2008 financial crisis, the Executive Direct of of Financial Stability for the bank of England (Haldane 2009) has attributed the lack of foresight concerning the likelihood of such an event to an oversimplified representation of rationality and behaviour in Risk Analysis models. How can a Risk analyst model human behaviour and rationality? Can Risk models account for biases and irrationality?
Knowledge	• In your view, how important is an organisation's Cybersecurity knowledge base for Risk Assessments? What sources could be used for knowledge base Supplementation/growth? • Can Knowledge strength be distinguished as part of the Cyber Risk Assessment process? How? • Are external information feeds available for the Cyber Risk Analyst? Are they useful? From this perspective (information feeds), how does Cyber Risk compare to other areas of organisational risk? • What role does Information System Design play in relation to Cyber Risk Management – more specifically, the production and communication of knowledge? • How can real-time Cyber Situational Awareness be integrated with Cyber Risk Management?
Uncertainty	• Is the uncertainty faced by Cybersecurity Risk Analysts distinct form other facets of organisational risk? If yes, how? • What are the main challenges which derived from the uncertainty faced within Cybersecurity Risk Modeling and Strategy formulation? • Significant efforts are made for the development of resources (products and services) designed to manage uncertainty within cybersecurity. On the other hand, the growing infrastructure of interconnected devices can indicate an increased attack surface, with new potential vectors of attack. In your view, how will the uncertainty that cyber risk analysts face evolve in the near/mid-term?

Risk	• In spite of some consistencies, the meaning of Risk and Risk Management can vary based on the context of its application. How would you define Cyber Risk? How about Cyber Risk Management? • Do you find quantitative or qualitative approaches to Risk Assessments as more suitable within the context of Cybersecurity? (if qualitative: How can subjectivity be mitigated? Are there any communication challenges imposed by the abstract nature of the topic? If quantitative: What is the efficacy of probabilistic techniques? How can data reliability be strengthened?) • The actual cybersecurity incidents track-record of organisations can largely depend on the specific threats they have faced, which blurs the use of 'number of incidents' as a direct metric of performance. How can 'good' implementations of Cybersecurity Risk Frameworks be identified?
Adaptation	• Adaptation, Resilience and Risk are tacitly presented as interlinked in a range of Cybersecurity policy initiatives. Based on your experience, are these concepts related? In what ways? • What is the role of feedback for the Risk Analyst? What is the basis of potential feedback? • Based on your perception, what are some of the current developments which are likely to push the utility of Cyber Risk frameworks forward?

Group 3: General Actors

- *Rationale of enquiry* (Bottom-up view): How general staff (i.e. with no direct Cybersecurity decision-making oversight) perceive Cyber Risks; How their perception of cybersecurity within their role relates to the assumptions of Group 2 and Group 3 actors.

Theme	Questions
Change	• Increased efforts from governing bodies, media coverage and a series of high-visibility incidents have raised the awareness concerning the potential effects of Cybersecurity breaches. Do you perceive cybersecurity to be of concern within your role? In what ways? • Are your computing choices (i.e. software selection) and behaviour autonomous, or are they the result of institutional policy? What is your perceived degree of freedom of choice concerning your 'cyber' behaviour, in relation to your role? • Have there been any noticeable changes in the norms, role, or day to day action due to Cybersecurity efforts/concerns?
Rationality	• As part of Risk Assessments, the various systems, roles and actors (employees) within an organisation are evaluated in order to identify vulnerabilities, and estimate the impact of potential breaches. In order to manage the complexity of this process, assumptions and models are often used. What aspects of your role, if any, do you perceive as prone to misrepresentation within a Risk Analysis? • Given its inherent dichotomies, such as system accessibility and security, Cybersecurity can rely on nuanced choices which balance the potential gains of an action with the potential costs/ramifications. Do you view intuition as a potentially effective selection mechanism for such choices? Rules of Thumb? • How would you describe the Cybersecurity climate/culture within the industry?
Risk	• Is Cybersecurity a criterion for your choices in technological behaviour? How can you validate a specific choice from a Cybersecurity perspective? • Have you ever noticed cyber vulnerabilities in the systems, processes or individuals that you interact with? Are you confident in your ability to identify and report relevant changes and anomalies? • How do you perceive the current sector-wide cybersecurity risk climate?
Adaptation	• A key pre-requisite for adaptation is the replication of effective behaviour. Within your role, how can one distinguish effective cybersecurity practice?

Appendix 4. Ethics Form

Attached as separate document in order to uphold anonymity requirements.

Appendix 5. A Risk-Centric Overview of Relevant Industry Standards & Frameworks

5.a) ISO/IEC 27000 Family

Overview – (International) Information Security Management Systems Standards;
ISMS: "consists of the policies, procedures, guidelines, and associated resources and activities collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintain and improving an organization's information security to achieve business objectives. It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks." (ISO/IEC /IEC 27000 2018:11)

Risk Conceptualisation: effect of uncertainty (deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood);

Context – Risk management as a 'Planning' dimension of Information Security Management Systems; Information Security specific implementation of 'Risk'; consistent with ISO/IEC 31000 – 'Risk Management' family of standards;

Risk management process (loop):
(based on ISO/IEC 27005* Guidelines):

- *Risk identification*: Assets; Threats; Existing Controls; Vulnerabilities; and, Consequences
- *Risk Analysis*: Qualitative (scale for consequences and likelihood); Quantitative (measures & data for consequences and likelihood)
- *Risk Assessment*: Relevant scenario considered based on previous dimensions; Outcomes assessed based on effects in asset confidentiality, integrity or availability;
- *Risk Evaluation*: Risk values compared to previously set evaluation and acceptance criteria
- *Risk Treatment*: Controls for based on risk modification (reduction), retention, avoidance, and sharing strategies; Yields residual risk.

Notes:
27005:2011 (second version)*/ Informed literature review, data collection, and framework development; Conceptually consistent with the third version of the standard.
27005:2018 (third version) – based on 'asset, threat, and vulnerability' risk identification method – no longer required by ISO/IEC 27001;
NIST SP 800-12 and 800-30 included in the bibliography of ISO/IEC 27005:2018;
Thesis discussion incorporates related standards:

ISO/IEC 27000:2018 – Overview and Vocabulary
ISO/IEC 27001:2013 – Requirements (Information Security Management Systems)
ISO/IEC 27005 – Information Security Risk Management (Guideline)

5.b) NIST SP 800(-39:2011/-30:2012) – Managing Information Security Risk & Guide for Conducting Risk Assessments

Overview: (US Based) SP 800 Series – "guidelines, recommendations, technical specifications, annual reports" addressed towards the "computer security community";
Guidance publications;
SP 800-39 'Managing Information Security Risk'
SP 800-30 'Guide to Conducting Risk Assessments' -- aimed to 'amplify the guidance' in SP 800-39, specifically concerning the Risk Assessment Process

Context: Risk management presented as Multi-tiered:

- Organisation View: Governance, Risk Executive Role, Risk Management Strategy, Investment strategies
- Mission/Business Process View: Risk Aware Business Processes, Enterprise Architecture, Information Security Architecture
- Information Systems View: Integrated Risk Management in Information Systems Lifecycle

Risk Conceptualisation: "A measure of the extent to which an entity is threatened by a potential circumstance or event"; Function of the impact of said event, and the likelihood of its occurrence;

Risk Management Process:

- *Frame*: Describe context, and establish a risk management strategy for the following stages;
- *Assess**: Identify the Threats, Vulnerabilities, Harm/Impact (if threats exploit vulnerabilities), and Likelihood;
- *Respond*: Develop organisation-wide response to risk frame – Develop alternative courses of action, evaluate alternatives, determine appropriate action, and implement the selected response;
- *Monitor*: Determine effectiveness of responses, Identify relevant changes to the information systems and their environments, verify that risk responses are implemented and compliant with relevant regulations;

Notes:

*Risk Assessment methodology further elaborated in SP 800-30, as a product of the Organizational Risk Frame, to include Risk Assessment process, Risk Models, Assessment approach and Analysis approach**;** Compatible with pluralistic risk assessment methodologies based on time frame, the complexity and maturity of the business process, the stage of the information system in its development lifecycle, and the sensitivity/importance of the information/information system;
References ISO/IEC 31000, 31010, 27001, 27005 – explicit goal for the 'harmonization of standards', to reduce burden for organisations conforming to both ISO/IEC and NIST standards;
No updates to the frameworks have been made throughout the duration of the study.

5.c) NIST Cybersecurity Framework (Framework for Improving Critical Infrastructure Cybersecurity)– 2014 (v.1.0)/2018 (v.1.1)

Overview: Risk-Centric Framework which presents a common structure for organising cybersecurity efforts through existing standards, guidelines, and practices.

Context: Primarily focused on, but not restricted to, critical infrastructure organisations. Entails three components:

- Framework Core – consists of concurrent and continuous functions: Identify, Protect, Detect, Respond, Recover; Each presents 'Categories' (function specific grouping of cybersecurity outcomes), 'Subcategories' (division of category into specific activities), and 'Informative References' (documentation to support each subcategory);
- Framework Tiers – describe the characteristics of the risk management approach chosen by the organisation. Consist of: 'Partial', 'Risk Informed', Repeatable', and 'Adaptive';
- Framework Profile – Alignment of the framework core with the organisational-specific risk context. Profile comparison (i.e. Current vs. Target) can underpin development plan.

Risk Conceptualisation: NIST SP 800-*: "extent to which an entity is threatened by a potential circumstance or event". Function of likelihood and impact of said event.

Risk Management Process: Describes risk management as an "… ongoing process of identifying, assessing and responding to risk". No specific process included; instead, the framework aims to be compatible with "a broad array of cybersecurity management processes", including ISO/IEC and NIST.

Notes: References include ISO/IEC 31000, ISO/IEC 27001 & 27005, NIST SP 800-39, and COBIT 5.
V 1.0 (2014) of the Framework informed the literature review and conceptual framework development. None

of the changes brought by version 1.1 (2018) are found to affect the validity/applicability of the sections referencing the framework.

5.d) COBIT 2019

Overview: ISACA Enterprise Level "I&T Governance Framework"/ Enterprise Governance of Information and Technology (EGIT); 'IT Related' Risk integral dimension of framework.

Context:

- Identifies Alignment to 'Major Standards' as a key principle for a governance framework, alongside it being 'Based on a Conceptual Model', and it being 'Open and Flexible';
- IT-related risk integrated within enterprise risk management (emphasis on holism);
- 'Risk Profile' alongside 'Threat Landscape' as an enterprise governance system design factor; Proposes IT 19 Risk Categories for establishing the Organisational Risk Profile;
- Integrates 'Ensured Risk Optimization' as part of the Core Model Governance and Management Objectives and Purpose.

Risk Conceptualisation: Implicit – "Risk management focuses on the preservation of value"; Contrasted with value creation

Risk Management Process:
Management Objective AP012 – Managed Risk*:

- *Collect data*: identify/collect data necessary for following risk identification, analysis and reporting;
- *Analyse risk***: gain 'substantiated' perspective concerning IT risk;
- *Maintain a risk profile*: inventory of risks and attributes (frequency, impact, responses), as well as relevant resources, capabilities and controls for risk items;
- *Articulate risk*: communicate relevant outputs to stakeholders;
- *Define a risk management action portfolio*: manage risk reduction opportunities as a portfolio;
- *Respond to risk*: timely response to materialised risk events.

* includes example metrics, suggested activities, related guidance publications, and detailed references
** consistent with ISO/IEC and NIST Risk Analysis: Likelihood/Impact per risk IT scenario, accounting for existing controls;

Notes: Includes references to NIST SP 800-37/53, NIST Framework for Improving Critical Infrastructure Cybersecurity, and ISO27000 family of standards
Distinctly elaborate guidelines; Emphasis on enterprise level performance.

Appendix 6. Data Analysis Excerpt

I. Table of the nodes generated through the coding process:

Name	Sources	References
des.Effective CS - Decision Making and Strategy	10	13
des.Awareness and Communication	10	22
des.CS in Sector	8	21
des.Institutional Risk Practices	8	26
des.Communication Strategies	7	12
des.CS Perception	7	20
des.Institutional Change	6	8
em.Attitude towards institution_leadership_culture	6	10
des.Knowledge in CS_Definition	6	8
des.Compliance	6	9
hyp.Knowledge_Problem	6	12
des.Rationality_Heuristics	6	8
des.ICT Freedom of Choice	6	9
des.Openness and Freedom	5	7

des.Adaptation and Adaptative Capacity	5	10
des.Feedback sources and strategies	8	11
des.HolisticvsMechanistic	4	6
des.Rationality_Bias	5	9
des.Role Transparency&Homogeneity	5	10
des.Partners and Collaborators	4	18
des.Risk - Effectiveness	4	11
des.Knowledge in CS_Validation	4	6
iv.Not-quite-there-yet	4	8
iv.Need to change	4	7
des.Uncertainty in CS	4	5
des.Pace of Change	4	4
em.Intuition_Positive	4	5
em.Trust_Lack of	4	5
des.CS Event Predictability	3	6
des.Role of Macro Bodies	3	6
des.JANET	5	8

des.Role of Macro Bodies_GDPR	4	7
des.[MACRO BODY]	1	13
des.[MACRO BODY] CCERT	1	2
iv.[MACRO BODY] Structure	1	3
iv.[MACRO BODY] History	1	1
des.[MACRO BODY] Process	1	1
iv.[MACRO BODY] Services	1	6
hol.PrivacyvsSecurity	3	4
des.Case Description	3	4
des.Anecdotal Evidence	10	58
des.Anecdotal Evidence - Vulnerability	10	29
des.Anecdotal Evidence_Computing Behaviour	7	9
des.Anecdotal Evidence_Threats	6	17
des.Anecdotal Evidence_EHS	3	3
atr.Role Description	8	13
des.Risk - Definition	3	3
des.Approaches to Change	3	3

des.Sector Comparison	2	3
des.Security Paradigms	2	2
des.Security Dichotomies	7	12
hol.Cultural Behaviour	2	2
too reliable [reliant] on… on computers	2	2
des.Defence Limitations	2	4
iv.Own Device	2	2
em.Emotions and Decision Making_Fear	1	1
des.Business Ecosystem	1	2
iv.Culture of security	1	1
iv.The system has to be robust.	1	1
des.Industry Change	1	1
des.ENT	1	12
iv.Reactive Service_Enterprise	1	1
des.Case Description_Enterprise	1	8
iv.ENT_own enterprise	1	2
des.Stakeholders_ENT	1	1

iv.Challenge_for_the_leadership	1	1
iv.Beyond IT	1	1
iv.Cyber Citizenship	1	1
iv.Business Architecture	1	1
iv.Tools in IT Department	1	3
iv.Challenge_education_training_awareness	1	1

II. Redacted* version of the matrix display;

*The structure has been simplified and adapted to fit the appendix format; Actual quotations were excluded due to research ethics constraints (approval for direct quotation reserved solely for case narrative) and space considerations; The excerpt reflects a working document designed for internal use, and maintains acronyms, references to other documents and notes, keywords, and interview material; A complete (transposed) version of a sample of individual nodes has been included in the Data Analysis chapter. Additional nodes and quotations (i.e. In Vivo/Descriptive for the Case and for the Actors) were not included in the matrix, as they address individual instances/require no context/are self-sufficient/are anecdotal; but they have been included in the case narrative where deemed appropriate; The corresponding research objectives precede entries (i.e. *1.*), and are further divided into subobjectives (i.e. *1.a)*); Each node is followed with a respective aggregate nodes entry, which has been excluded from the table format.

The redacted headers are consistent across the tables, and as a result have not been copied into individual nodes. These are:

Theme	Interviewee	Point (Des - An)	Notes (Entry)

1. Identify how Knowledge relating to Cybersecurity is produced, used and adapted at various levels within an organisation

1.a) How Cybersecurity Knowledge is Defined;

Knowledge in CS - Definition	Charlie	AN: Knowledge unit varies based on audience	Collectivist pragmatic perspective of knowledge; 'what it looks like' heavily determined by dissemination and assimilation mechanism. No universality in specialisation-based environments, instead contextuality is proposed. Practical examples favour narrative.
	Val	AN: Pragmatic collective/relational view of knowledge. Beyond that, "not important"	(abstractly individualist) Collectivist pragmatic - relational perspective of knowledge. Given the high level of DM, individual issue depth of awareness is delegated. High level context and 'relevant' awareness are instead favoured, which entails a reliance on organisational structure/hierarchy and communication strategies and mechanisms.

	Kendall	AN: Knowledge as a function of experience, intuition and action. "Hands on" & "Grey matter" (Abstraction)	Individualist pragmatic epistemology of operational actor (to be contrasted with DM's collectivist view). Knowledge as personal enabler of action -- function of previous experiences that were internalised to form intuition, which is deeply valued by interviewee. (! = Actor definitions of knowledge are individualistic - vs DM.)
	Ash	AN: Pragmatic, collective/relational, risk based.	Emphasis on probabilistic knowledge vs. truth "where breaches are likely to come". "Minimise the Unknown Unknowns" which is a theme. The UU paradigm only works on a foundation of pragmatism.
	Alex	AN: CTO: Pragmatic, Collectivist, Risk Based. Functions of Knowledge in CS: Threat analysis (Outsourced), Internal operational awareness, and Paths of action/response.	The description follows the T-V-I+Response Risk Management structure. This patterns seems to indicate the permeation of risk constructs as heuristics in security thinking. Again, collaborative, pragmatic. Distinct emphasis on awareness of business functions for vulnerability understanding, impact estimates and adequate prescriptions. This emphasis seems role-based. Emphasis on regulatory knowledge indicates adaptive separation, yet it is still bundled.
	Rudy	AN: IS/CS Practitioner Knowledge - Risk Based, Pragmatic, Collectivist	Collectivist pragmatic epistemology, More specifically, knowledge is presented as enabling defence, and entails awareness of threats, vulnerability mitigation (training and policy development), and process (how policies should be adhered to)

Notes: The most common definition tends to be collectivist/pragmatist - but this seems skewed by the sample; Managers'/DMs responsibilities tend to have a meta-operational dimension to them, and involve coordinating a multitude of individuals and capabilities; In contrast, a less KI/highly specialised role would entail localised beliefs and abilities. However even such a role requires a context, and entails delegation of other tasks.

1.b) How Cybersecurity Knowledge is Validated

Knowledge in CS - Validity	Charlie	AN: Valid knowledge must be 'Up to Date'	Temporality as a criterion for knowledge validation; Interviewee's definition of knowledge is again pragmatic, "what could happen? How do I prevent it? What do I do if it does happen?" - this anchoring to action makes particular 'knowledge claims/objects' bound to a spatio-temporal context. I.e. are not abstractly true/consistent in their ability to answer the questions and lead to action
	Alex	AN: Knowledge validation - An adaptive iterative process built on feedback. External feedback is encouraged.	Process outline: The structure of the process of validation is described, as iterative, collaborative and bias-mitigative through the involvement of a 'different set of eyes'. Emphasis on empirical testing/feedback, communication, adaptation and iteration.
	Ash	DES/AN: Knowledge validated through Source	Trust in source as a heuristic mechanism; proxy validation (trust the source -> trust the information -> trust the knowledge). The concept is also indicative of consideration to frameworks/tools as the foundation of inference.

	Val	AN: Knowledge validated through Trust/Source	Again, trust as a criterion to validate knowledge strength. Similar to Ash, another senior DM role. Could be quantified based on a perpetually training model. I.e. X employee/Decision maker has a 'trust factor' of…

Notes: Value of knowledge validation is undisputed amongst the interviewees. Methods for validating knowledge include: consideration for temporality and contextuality, iteration and collaboration with external entities, empirical testing, trust in source;

1.c) Role of Knowledge: Uncertainty in Cybersecurity

Uncertainty in CS	Charlie	AN: Uncertainty in CS is Distinct due to Speed and Breadth of impact	Uncertainty due to Pace and Breadth of impact (variance). Ties in Knowledge with Change as Topics. Also consistent with risk/systems theory assertions concerning the role of risk in high uncertainty.
	Rudy	AN: Unknown Unknowns are the big challenge	Uncertainty due to lack of internal visibility and deviation from established protocol.
	Ash	AN: Most threats are predictable. The unpredictable ones are 'likely to catch you' - UU.	This ties knowledge with mitigation against Unknown Unknowns.
	Alex	AN: CS Uncertainty 'Special' due to potential impact of UU	This validates the Knowledge Problem hypothesis. It also entails DM in CS must be conducted under DU

Notes: Uncertainty in CS distinct due to: Speed and breadth of impact, scope of 'Unknown unknowns', and their impact, and consequence of unpredictability (Ash)

CS Event Predictability	Val	AN: Events predictable at a high level 'i.e. Something will occur'. Predictability inversely proportional to detail	Ties in to the UU narrative - hit by the threats that were not predicted. Predicted vs. predictable are distinct.

	Rudy	AN: IS Staff: Attacks are non-homogenous, very few patterns;	The patterns that do exist indicate emergence: i.e. ratio between attack types in a taxonomy, which is indicative of complex system macro-behaviour. Not linked in the sense of traditional causality. The perspective is also different from Val's, and anchored in a more operational interpretation of CS DM. Given lack of homogeneity/linearity - DU is present, and this leads to reliance on Assumptions and Intuition. No historical consistency. Regularity vs. Patterns.

2. Critically analyse the role and epistemic requirements of Cyber Risk Management

2.a) Change and Cybersecurity

Pace of Change	Charlie	DES: High pace of change; AN: Important for management approach - Rigidity ('Security Conscious' Approach) is not effective	This also ties in with the panarchy argument - the institution does not exist to be secure, but to add value. This generates a tension between its primary value adding activities and security. Senior management which are risk + change adverse are perceived unfavourably given the exogenous pace and type of change. Consistent with Val's 'do everything safely' paradigm.
	Val	DES: Very fast pace of change. Trying to keep up is the issue (with CS). AN: Challenge - prevent CS from being a disabler of adaptation.	Consistent with Charlie's point. Industry is rapidly evolving (KI), and both Threats and CS practices can inhibit an organisation's adaptive practices, through policies, processes and technologies. Dichotomy between security and 'agility'
	Rudy	DES: IS Staff - Suspicious 'never sure' of knowledge, given pace of change.	As the attributes of Risk components are rapidly changing in the organisation, this affects the knowledge base, and the confidence in inferential procedures which rely

			on it. This also shapes 'institutional risk practices'

Notes: Consistency in the characterisation of pace: very fast, implications on knowledge, analysis, adaptation, and management approach

Institutional Change	Eli	DES: Increased Management Pressure, Training, and Perceived Threat Activity	The attitude of operational employees towards CS policy and the institution is also of interest. In this case, it seems to be very positive - which ties in well with the participant's declared preference towards security vs. openness. The participant also mentions explicitly he trusts the institution and its systems.
	Kendall	DES: Actor: 'Massive Changes', Increased Awareness; AN: 'Buzzword', Institution 'Over Cautious', Lacking the required 'Professionalism' to implement strategy	In contrast to Eli, Kendall does not have a positive view of the institution's CS efforts and pressures, nor of its capabilities. At the same time, he views CS as a constant which cannot be 'solved', and does not trust technology. He cares about 'getting job done' regardless of process. Themes include 'trust' + IV.too much reliance

	Remy	DES: Technical Actor: Institutional Change driven by Incidents and problems (internal and external); AN: New senior members indicate a change in stance on CS, 'taking security much more seriously'	The interviewee sees 'the industry' as having more IPR to protect -- sector comment. This indicates a low visibility of the data pockets that Rudy mentioned. The recruitment of a security-focused head of IT appeared as a theme in multiple interviews (i.e. Charlie), and was perceived as an 'interesting' turn of events, as the employees expected changes.
	Sage	DES: Actor: completely different from 3-4-10 years ago. Continuously changing topic puts learning pressures.	Interesting claim in relation to Kendall, who has a very substantial history within the organisation, having joined >20 years ago.
	Rudy	DES: Increased reliance on AI/ML technologies and solutions for operational CS.	The availability and value of new solutions which employ automation, machine learning and artificial intelligence has also been highlighted by Alex.
	Rudy*	DES: Any system change modifies the architecture - brings new risks	Interviewee highlights an analytical limitation, based on change: any system change reflects in the architecture and modifies the parameters of existing risk assessments. Given the institutional scale, such changes occur with high frequency.
	Fin	DES: Big concern; new procedures, progress with formalising CS posture	The actor has been with the institution for two years

Notes: Significant perceived changes in the institution which include: increased management pressures, training, procedures, formalised stance/policy, and more active visible threats, awareness, 'over-caution'; leadership recruitment patterns (IT), reliance on automation, AI/ML and technology for defence, continuously changing risk landscape;

Sector change	Brooklyn	DES: Amount of incidents (at an industry level) has been growing YOY. DDoS increased tenfold over three years. Huge attack surface	Oversight body CS role.	*At a sector level, significant increases in threat activity; varied response from individual institutions based on their interaction and awareness.*

Notes: At a sector level, significant increases in threat activity; varied response from individual institutions based on their interaction and awareness.

2.b) Adaptation and Feedback

Adaptation and Adaptive Capacity	Charlie	AN: Adaptive is Key: Awareness, Speed and ability of response; [Not there yet]. Adaptation seen to entail Gathering and sharing of Knowledge through the wider value network. Change manifested in systems/policy. Etc.	Very positive view of the potential of 'adaptive cyber risk management' - not necessarily based on exposure to the specifics of such an approach - only on briefing documents offering a high-level representation of the research narrative. Also presents adaptation as a function of knowledge, and ability to produce relevant changes at appropriate scale and pace.
	Val	DES: Both sides (Threats-Vulnerabilities) are inherently dynamic; An internal dichotomy also exists between preferred pathways - Leadership must reconcile/manage/compromise on such tensions	The point on the dynamic between individuals who push for security vs. individuals who push for openness is also highlighted by Charlie in the description of witnessed approaches to CS decision-making. Attack-defence engagement is also inevitably dynamic, and largely zero-sum, raising the issue of

			adaptive response on both sides.
	Ash	DES: Constantly seeking in order to stay on top of risk; Awareness of limitations in knowledge	Loosely ties adaptation with knowledge and risk. Only does so at a pretty obvious level.
	Alex	AN: Adaptation 'learn by doing' while maximising sources of potential feedback, and, thus, mitigating bias. AN: Resilience is foundational, "The key to doing risk is adaptability" - Pace of change imposes adaptation as a selection criterion.	The overarching pattern across the theme is a highly favourable perception of adaptivity/adaptation, especially in relation to knowledge and risk. The dynamics of adaptation are tied to: 'lack of certainty' - awareness of unknown'; 'maximising feedback streams'; 'balancing pace and ability to respond'; 'acquiring and deploying knowledge at an adequate pace, given the local parameters of the problem', ' an ability to manifest intent, in accordance with problem perception - i.e. perception of selective pressure appropriately translated and implemented into action'

Notes: CS seen as an inherently continuous process; very favourable view of the maximisation of adaptivity as an objective; Activities include: gathering and sharing knowledge through the wider value network, continuous 'scanning' and awareness optimisation, 'learn by doing while maximising source of potential feedback', and re-positioning oneself on key dichotomies – role of leadership.

Feedback sources and strategies	Charlie	DES: Importance of highlighting near misses/small occurrences, help policy learn from where breaches have occurred. Importance of awareness of what needs to be reported. DES: Adaptability based on Sharing and Knowledge. AN: Needs to be a knowledge gathering and analysis function exploring policy analysis, events, networking; used to adapt risk management policy and tweak systems	While this overlaps with a previous use of the second part of the quote - feedback and adaptation go hand in hand. Charlie finds that there's a need for a function to integrate feedback and perpetually adjust policy and systems in response. This function fits the characteristics of an adaptive information system/knowledge system.
	Eli	DES: Feedback for operational actors is internal, and function oriented	IT Guys' are expected to guide behaviour internally. This indicates an intra-organisational point of reference, and re-emphasises the point that knowledge has to be translated based on its audience. Selective pressures are manifested between layers of a hierarchy, and generally do not skip stages
	Kendall	DES: Feedback - Use the experts	Again, operational actor with the same outlook as Eli. The core difference is that Kendall wants to address the experts, and in his examples, he mentions academic colleagues with expertise rather than members of the IT function. Nonetheless, there is a theme of operational actors looking at the institutional structures and functions for a clear cut direction of behaviour. There is also an implicit assumption of right and wrong, and of homogenous expertise concerning what needs to be done in a given situation.

	Brooklyn	DES: [SECTOR BODY] Feedback Provided	Covers the various methods of feedback and information sharing undergone by [SECTOR BODY] for its clients.
	Val	DES: Strategic feedback comes from the confrontation of opposing interests, and their representatives.	Unlike other levels, the seeming role of leaders in CS is to reconcile a position on dichotomous spectrums that enables the maximised generation of net value. As the developers of policy, their pressures are less about compliance (unless liable for certain measures in relation with macro-bodies) and more about top-down direction setting. The content of the feedback must, thus, be already synthesised and presented within the context of strategic objectives - making specific points of action and policy less important than the holistic view. Key tensions and concerns seem to arise from dichotomies more than anything else. The sense of 'the right answer' had by operational actors is not apparent
	Rudy	DES: Technological Feedback and Monitoring essential for Technical Actors. Development of heuristics	

	Alex	DES: Hard measures - Business outcomes; Soft measures - sentiment and perception of service; External feedback and benchmarking. Openness as key for gathering feedback	IT (Functional) leadership's view of feedback reflects an intermediary point between Val and Rudy. Views CS objectives as highly pragmatic and nested within the grander IT strategy, which is also the source of KPIs. External network and collaborations seem more accessible based on functional divisions (i.e. IT in HE).
	Ash	DES: ENT - scale shapes available feedback; Absent dedicated resources, informal networks are seen as the most viable source of feedback. Subsidiaries rely on the university. No systemised approach to intelligence gathering and DM.	A centralised Adaptive Knowledge function could also be used to selectively support subsidiaries and partners exposed to the same causal forces. The link between sources of input and resources is evident. Informal networks are favoured, and seen as powerful sources of insight (this should be reflected in modular KCs).

Notes: Feedback: level dependent; importance of format and awareness of what needs to be reported in order to lead to change in behaviour; feedback for actors is internal and function oriented (i.e. IT); Macro-bodies like [SECTOR BODY] aggregate and provide feedback as a service; technological feedback is essential to calibrate policy and positioning, feedback in terms of hard measures (business outcomes) and soft measures (perception/sentiment); 'Openness as key'; Scale shapes available feedback – ENT

2.c) Risk Analysis: Actor Behaviour

Role Transparency & Homogeneity	Eli	DES: Policy and Process Adherence Go Hand in Hand	The overall characteristics of the interviewee are noteworthy, including the strong confidence presented in the institution and its ability to ensure security, and a preference for security over openness when presented as a dichotomy. The interviewee also primarily engages with teaching - a very mature activity in the

			institution. This maturity could also be reflected in the corresponding processes.
	Kendall	DES: Non-adherence to process and procedure to 'Get the job done'	Kendall is altogether different than Eli, having little confidence in the institution's ability to deal with the challenges posed by CS. He presents his behavioural variability as useful for the wellbeing of the business sub-unit, and objects to the depth of some security practices, i.e. spam filtering. Unlike teaching, the role is less mature, and thus the processes are less likely to provide an accurate portrayal of the day-to-day requirements .
	Remy	AN: A technical perspective of the likelihood of homogenous behavioural patterns.	The size of the organisation is presented as an indicator of how unlikely behavioural homogeneity is for predictive purposes. Part of this is attributed to a vast capability variance, and the nature of academic openness as a sector specific challenge.
	Sage	DES: Formal processes and descriptions are in tension with the top-down dynamics (policy and strategy) and bottom-up (changes in) nature of the work ; require an understanding of the business in order to be comprehended	Relevant as it sets a conditional foundation for disciplines such as enterprise architecture. Understanding risk is also predicated upon understanding the asset-vulnerability-impact dynamics. Staff behaviour is central to that.

	Fin	DES: Predictability depends on process - inversely proportional to Knowledge Intensity	Admin and teaching are seen as trivial, routine-type activities and are thus more likely to be predictable based on an understanding of the process. Research is different.

Notes: Process adherence and role transparency seems to vary based on personal perception, culture, role maturity/knowledge intensity, accuracy and understanding of the role within the context of its representation; Effectively employing this knowledge (i.e. business architecture) is also affected by organisational scale, i.e. Remy

Cultural Behaviour	Sage	DES: Loads of things that we are doing different in the UK	The actor perceives UK HE to provide less 'freedom and flexibility' than other universities. This also affects adherence to formal policy from staff members that are not from the UK. HE is highly multi-cultural, so this issue of cultural variability could play a larger role than in other sectors/industries.
	Fin	DES: 'Freaked out with procedures and bureaucracy'; Not perceived as effective based on breach occurrence.	This echoes the previous argument - multiculturalism shapes how policy is perceived and followed. As a secondary point, the actor seems to see 'being freaked out' with policy and procedures as ineffective for improving the overall security stance.

Notes: In the context of a prescriptive model, culture is not distinctly useful, given its ambiguous boundaries and limited malleability. Instead, (explanatory) awareness of the potential role of culture can help in the development of localised heuristics for procedural deviation likelihood. Data on Uni X staff/student origin and nationality available in 'Additional Data' folder

Intuition	Kendall	DES: Intuition - Extremely Valuable	Intuition is deemed as explicitly essential in decision-making, and in Knowledge (tacit). Furthermore, it is equated as the product of experience - which the participant benefits from.

	Remy	DES: "My intuition - good; others, clueless"	Again, explicit trust is placed in the value of intuition in decision-making. Like Kendall, Remy perceives his own intuition attuned and relevant, which is contrasted with 'other people'.
	Rudy	DES: Intuition is part of formal risk analysis. Not explicitly labelled as such; Communicated through 'vague language' as a way to reflect the lack of certainty. 'Hard to define'	The value of intuition is also perceived by IS RM participant, who, again, has a positive view of his ability to implement it effectively. However, intuitive 'gut feelings' are not communicated as such, and instead are masked through communication strategies, i.e. wording choices and phrasing that are not particularly precise. Accuracy vs. Precision in phrasing risk claims.
	Fin	DES: Operational actor computing choices - rational, not intuitive.	The nature of operational actor decision-making in relation to CS seems to be distinct, and more surface-level. As a result, the necessity of intuition is not explicitly recognised. The potential division over the semantics of the terminology is noteworthy.

Notes: Generally positive view of intuition as a source of CS DM; Part of formal risk analysis, but not made explicit; communicated through vague language to reflect lack of certainty

Rationality_Heuristics	Charlie	AN: Heuristics - Useful; at an institutional level, they require centralised data/communication; This is not present at the time of the interview	The interviewee is familiar with the role of heuristics in the decision-making (unlike most other participants), and perceives this to be positive, through the effects on individual attitude towards risk. However, an argument is made that at

			the time of the interview, the absence of a centralised information sharing function made the idea of institutional heuristics inapplicable. !Need for specialised, centralised information acquisition and sharing functions
	Remy	AN: Individual heuristics are a useful baseline for protection	Generic answer. Individual heuristics are seen as beneficial when part of a broader range of defensive 'tools'
	Sage	DES: Example of Security Heuristics used; Indicative of the low direct scope of concern, and awareness.	The participant was not aware of the notion of heuristics, so the answer seems post-hoc, not necessarily reflecting a voluntary approach. This lack of awareness might be attributed to the narrow nature of CS decision-making for an operational actor (given contrast between category 1 and category 3 awareness).
	Alex	DES: Heuristics are essential (for DM) given scale of operations. Perceived value of heuristics and machine learning	Heuristics are correlated with informational volume - a view that is consistent with the literature on the topic. The development of appropriate heuristics for operational cyber defence is seen as part of the future defence strategy, when coupled with machine learning.
	Ash	AN: Heuristics are 'pragmatic'; way to cut cost.	The more cost-oriented focus of ENT is reflected in this answer, which is consistent with Alex's view, but has a different justification. So, the scale is less of a concern (ENT infrastructure is significantly

			smaller), but cost is prioritised. Different driver for the pursuit of efficiency (cost) vs. effectiveness (scale).

Notes: Also worth noting that Heuristics and Biases are totally disconnected in the stance of the participants, at least explicitly.

Rationality_Biases	Charlie	DES: Bias not explicitly taken into consideration. DES: Broad capability gap in CS for Decision-makers. AN: It would be useful to consider bias	The participant highlights that decision makers across levels vary significantly in their skills and awareness in relation to CS, and attributes these capabilities with inherent bias/lack of awareness. !Useful for a system to highlight bias.
	Brooklyn	DES*: Industry level tendency to under represent risks pre-breach, and overestimate it after an incident.	The observation is in accordance to the theory on R&B. It is not based on the case itself, but on tendencies observed through direct exposure at an industry level.
	Val	DES: Biases seen all the time (in CS). They generate dichotomies. AN: Exposing and managing these is the role of leadership	For leaders, supporting any view when expertise clashes is strongly dependent on the systemic effects of the existing knowledge.

	Rudy	DES: No perceptual homogeneity in (subjective) risk assessments. DES: Current (institutional) Risk Assessments do not account for biases and 'irrationality'	Important to notice the difference in nuance when defining bias across participants; !mitigating for 'irrationality' and bias is perceived as desirable
	Ash	DES: Enterprise branch is cost/profit driven, with less financial buffer. 'Bias' vs. prioritisation/incentivisation	Reflects very well Val's description of bias; the heavy emphasis on cost can shape the perception of what is required from the perspective of security. Existential selectors on finance vs. security.

Notes: Variability in defining bias, but the pattern of viewing it as a concern, and as unavoidably present in decision-making is consistent. The idea of existential selectors on security distinguishes higher education as an area of emphasis versus other industries.

2.d) Cyber Risk and the Knowledge Problem

CS Dichotomies	Charlie	DES: Tension in Senior Management perceptions of CS, and across the organisation. 'lockdown vs. lackadaisical'	This tension feeds into the bias discussion, and Val's arguments on the challenges faced by leaders. It also justifies centrality in informational availability. Phase tension; 'Security through openness' as a personal stance

	Eli	AN: "balance is very important"; "Security trumps openness"	This is antithetic with the overall tone and view of Charlie who pushes for openness as a way to maximise security - by minimising what defence efforts are concentrated on. It seems to be a cultural attribute, and reflects a point on the continuum.
	Remy	DES: SysAdmins, Devs and Programmers 'take [CS] very seriously'; Non-technical administrators … 'awareness […] not great', and face organisational pressures which lead to 'pragmatism' and compromises. User awareness also perceived as low.	Remy is technical in his capabilities. Perceives technical capabilities, and awareness as a determining factor of the stance on the security - openness continuum. Highlights how technical functions and decision making may differ from broader organisational functions in that they are single goal driven - i.e. secure system, which can conflict with the numerous other objectives and tensions manifested within the organisation as a whole.
	Val	DES: Very quickly, you get compromises about openness and safety'; These are moments when speed of change and 'cyber' grind together. DM is about finding the right level.	The dichotomy is presented as continuous. The pace of change is brought into the discussion, as key when facing a crossroads on openness vs. security. Actually being able to determine what is 'acceptable' relies on assumptions, within the case, this seems to boil down to trust and direct communication, which does not scale well.

	Alex	DES: Fundamental tension between ideas of security, data protection and the university culture. "It's how you actually draw the line"	Supports the panarchy view, and the knowledge problem perspective. So does the previous point.
	Ash	DES: Organisational functions personify the dichotomy	While important, security is perceived as an operational inhibitor.

Notes: Dichotomies and tensions, both internal and external, are central to the discrepancy between an abstraction of organisational behaviour and its real manifestation; CS is underpinned by fundamental dichotomies

Risk Definition	Charlie	AN: Risk = (likelihood x impact) negative event	Textbook definition.
	Rudy	AN: Cyber risk = Vulnerability	Vulnerability centric definition of risk
	Alex	AN: Threat-Impact	The risk is the threat, and it is a threat because of the impact it can generate

Notes: Together, the three definitions cover the full spectrum of reasonable definitions: likelihood, threat, vulnerability, impact.

Risk Effectiveness	Charlie	AN: Risk Effectiveness is meaningful to people.	The point made relates to two dimensions: effectiveness and suitability of policy and measures, and meaningful impact for the actors within the organisation. The latter is underwhelmingly considered in risk theory.

	Sage	AN: 'tick boxes' i.e. policy and procedures do not equate 'responsibility'	An actor perspective on the point made above: 'tick boxes' are limited, and conditioned by the impact of the topic on the individual actors.
	Rudy	DES: High variability in perception of likelihood and impacts; ISO27001 (very very simple). AN: "Would love some sort of consistent algorithm where you could asses a data base, say, and put a figure, a number on the risk based on number of records held, how sensitive the data contained is, who would have access. Nothing like this out there. AN: Good risk management implementation - cannot be defined. Only good until breach	The point will most likely be repeated in the need to change category, but Rudy describes IS Risk Analyst requirements to overcome excessive subjectivity and perceptual heterogeneity of risk assessments. Consistent with Remy, anecdotally arguing that the role and capabilities of an individual are likely to shape their view of CS.
	Alex	DES: Effective Risk must be communicated in 'business terms' - job of IT leaders. Must have empathy with business rather than pure IT: panarchy (prev Remy) Risk is a 'coms tool', (implicit - low accuracy) and helps prioritise; Good risk management: hierarchical, from	Given simplicity, Utility of risk as 'communication and prioritisation' tool, rather than knowledge formation or deep uncertainty management. Importance of anchoring CS in business risk, hierarchically.

		process, to IT service, to systems, to business risk	

Notes: Risk as a communication, and prioritisation tool; low level inferential load; Impactful communication and risk; simplistic and pluralistic in likelihood; importance of understanding impact (business risk) appropriately, need for consistency in analysis – Rudy

Institutional Risk Practices	Charlie	DES: DM use of risk in institution 'individual and contextualised'. 'Not seen a general approach towards risk', only copyright, DPR, IP, ethics, Health and Safety	The maturity of risk processes tends to revolve around mature components of the business. Cyber might be seen as an enabler of those, rather than a standalone dimension.
	Brooklyn*	DES: Industry level - interest in formal frameworks granular and localised. ISO/Cyber Essentials pursued for small scope tasks. Accreditation criteria conflict with academic openness.	Organisation-wide cyber risk framework proliferation is a lot lower at an industry level than other, general reports would indicate. It also depends on how 'risk frameworks' are defined - ISO/IEC vs. just a localised risk assessment. The maturity of cyber risk practices is seemingly low at an industry level. This might also indicate, as with the case data, using risk constructs for communication and low-level prioritisation more than anything else.

	Remy	DES: Risk is used to contextualise the CS occurrences and awareness. In spite of this, technical staff does not reference any sort of formal structure. Risk as a heuristic	What drives the point of risk utility is the finite set of resources which underpin defence efforts. Contextualising and comprehending threats within the wider context of the business is essential for structuring a pro-active, or adequately reactive approach.,
	Val	DES: A colloquial description of risk planning and response strategies.	No formal structure is mentioned but it is clear that decision-making at the highest level is risk-informed, at least in terms of framing and contextualising.

	Rudy 1	DES: A description of the Risk Assessment process from the IS FUNCTION. Audit vs. health check. Extends onto third parties through privacy impact assessments, and legal framework establishment	In case, the IS Function seems to be the function in which Information Security Risk is taken into consideration. ITS seem to focus on 'cyber' . No proof of awareness concerning the opportunities presented by a centralised knowledge base, including for 'strength' determining within risk assessments, etc.
	Rudy 2	DES: Centralised 'repository' - Work in progress; Contains: risk assessments, third party compliance, due diligence and instant reporting. DES: ITS - own security work. DES: Knowledge 'strength' not part of assessments.	

	Rudy 3	AN: IS likely to be similar across sector. 'case' set up different than other universities, IS FUNCTION outside of IT. IS Risk analysis conducted by 'non-IT people'	
	Alex 1	DES: two streams of risk: university level - policy and risk assessment. IT risk assessment - different risks, system vulnerability and likely hacks.	Differentiates the IS Function Risk analysis which falls under the first stream from the IT stream. Not fully clear how the two are different, as IS entails network monitoring and defence, in addition to non 'cyber' measures of defence.
	Alex 2	DES: understanding how the business operates is essential to quantify risk. DES: IT Risk assessment done in impact and likelihood - two numbers for each, one through nine, multiplied	The description of the IT Risk analysis practices supports the previous view of no formal framework, but risk driven efforts of understanding and structuring defences.

	Ash 1	DES: ENT global Risk Analysis - Uni based, with no formal feed down. Two levels of security: network integrity and security, and student personal data.	Lack of certainty is presented as a driver of agility and adaptation. Environmental scanning and knowledge acquisition/validation is conducted informally. No formal feed-down from the university, in spite of perceived reliance. Risk frameworks are seen as potentially dangerous if they generate over reliance - ties in with uncertainty and predictive power (ontology).
	Ash 2	DES: Reputational Damage, biggest concern for ENT. No formal risk framework; AN: The bigger the framework, the larger the likelihood of overconfidence in its output - too formulaic/reliant on something structured and mechanistic	

Notes: Difficult to summarise; re-read in entirety

Effective CS - DM and Strategy	Charlie	AN: Effective risk: Contextual, appropriately communicated, part of a conversation with stakeholders, clear action-plan communicated to key people.	Communication is presented as central to effective risk management - a point that is consistent with the idea of organisations as coordination-driven meta-entities with knowledge networks.

	Eli	AN:'Actor' - Effective CS - policy and procedure, supported by training and awareness, coupled with periodic stress-tests	A lot of emphasis on system resilience and systemic properties. Explores CS as a systemic phenomenon. Implicitly, it delegates/spreads the role or responsibilities of the individual in this context to wider structures.
	Kendall	AN: Effectively communicate and leverage expertise	A different angle on the Charlie view of communication as central for strategic efficacy. Reflects awareness of a lack of direct expertise
	Brooklyn*	AN: All-encompassing, beyond technical, holistic. Coupled with awareness.	
	Remy	AN: strategy starts with understanding specific level of risk; focus of senior management, training and education, sensible policies, balancing risk with cost	A broad range of activities predicated upon the idea of balancing risk with cost - two dimensions of the 'knowledge problem' narrative.
	Val	AN: Enabling safe value generation	Ambiguous - supports the panarchy hypothesis;
	Rudy	DES: Policies (great) exist with built in ISMS, 'not applied - people don't even know the way they should be behaving' DES: Challenge education and training	Goes back to Charlie's point on communication. The existence of policy, regardless of its quality, is irrelevant if it is not able to guide actor behaviour. This requires communication, contextualisation, awareness --> knowledge.

	Alex 1	AN: Efficacy requires the integration of technically capable/oriented individuals in the business, to fully understand measures and impact.	Business architecture is central to the definition of an effective IT-based cyber strategy. Issues with business architecture (partially addressed in emphasis on integration rather than just blindly using documentation and procedures)
	Alex 2	DES: Integration to business models and operational lifecycle. Tied to the IT strategy, and therefore Corporate Strategy. DES: Process of formulating the strategy	The process of CS strategy formulation, which includes interviews with stakeholders, and is seen as nested in the IT strategy, which is nested in the corporate strategy, and overall business risk. CS - 'same questions' into different 'focus space'

Notes: Operationalising strategy? Communication and policy; implementation holism, education and awareness. Purpose is coordination by minimising knowledge asymmetries on relevant topics

Not-quite-there-yet	Charlie 1	DES: 'Adaptivity' will be key; Need speed of response and awareness. Not there yet; AN: Currently far behind that conceptualisation due to limited understanding of risk	Your word 'Adaptive' is going to be really key - Demands for Adaptivity maximisation. This would be materialised in the form of increased awareness, better internal communication, faster response, a stronger understanding of the scope of existing knowledge, and risk faced.

	Charlie 2	DES: Holism in approach is desirable, but not currently practical given maturity of CS in the case. Holism should be 'end goal'	The idea of holism vs. mechanism for the conceptualisation of CS has a series of implications for the analytical granularity and scope of conceptualising the problems perceived. Any attempt at holistic approaches presupposes an exploration of both top down and bottom up phenomena. Also, communication structures so that feedback can be effectively communicated amongst levels of the hierarchy.
	Rudy*	DES: 'Wish' there were a way to deal with non-linearity mitigation	
	Alex	DES: Currently immature in the 'CS' space. AN: Knowledge validation - a concern; tied to maturity	Knowledge validation as a capability; The perpetual classification of the organisation as immature in relation to CS raises the issue on what are the main indicators of maturity - highly technical organisation, dedicated functions both inside and outside of IT, concern and debate at board level on the topic, explicit know-how, unique opportunities (i.e. Ethical Hacking) students, accreditation orientation at an individual level, profitable and investment-oriented, numerous layers of support, including macro-bodies like [SECTOR BODY].
	Ash	DES: ENT Small organisation - depends on security expertise of parent; 'we'd love to have someone (sic) scanning the horizon'	In this context, the lack of dedicated structures and staff is attributed to organisational size, and these are presented as desirable attributes.

Notes: Current systemic approach not optimised for adaptivity due to limitations in coordination and awareness (communication, speed of response, and understanding of risk as an expression of internal and external obscurity); An effective holistic conceptualisation of CS is tied to the maturity of efforts; Difficult to manage Non-linearity; CS Immaturity manifested in knowledge validation limitations; in ENT, CS is non-core for financial growth - would like dedicated scanning function;

Conceptualisation Granularity: Holistic Vs. Mechanistic	Charlie*	DES: Holism in approach is desirable, but not currently practical given maturity of CS in the case. Holism should be 'end goal'	Both quotes used for previous theme as well.
	Brooklyn*	AN: CS Strategy must be holistic	
	Alex	DES: IT Strategy Approach - more 'holistic' - Risk based is the platform for holism; vs. Gap analysis. AN: Can't get too hung up on [Risk Assessments] - given mechanistic scoring which can hide meaning.	The notion of holism is not perceived consistently across actors. Alex sees current conceptualisation as holistic, unlike Charlie. Each justify their view. Furthermore, Alex argues that 'risk based' is the holistic alternative to the mechanistic gap analysis per system.
	Ash*	AN: too much reliance on something mechanistic [like a risk framework] can increase complacency/rigidity.	Again, quote previously used. Ash sees formal frameworks as potentially counterproductive given the potential scale of their output which makes it easy to miss relevant phenomena. Could be why no formal frameworks are pursued at an institutional level. Ash also argues that, for ENT, more structure would be beneficial in relation to CS.

Notes: Perceptions on how to define and employ an adequate level of conceptual granularity vary depending on role;

Awareness and Communication	Charlie	DES: Because you don't know about threats, […] not enough information to change your heuristics. [Adaptation - Knowledge Problem]; AN: Education and awareness are essential for behavioural change.	Knowing about threats and the internal levels of awareness and types of behaviour encountered are both key for the pursuit of effective adaptive behaviour. Throughout the interview, Charlie highlights a rationale for the Knowledge Problem narrative, and the maximisation of Adaptivity. Part of that is underpinned by education, awareness, communication and openness.
	Eli	DES: Actor - Limited awareness of the scope of CS; Self-perceived efficacy in awareness and relevant capabilities; Perceives existing training as sufficient, increasingly substantial, compared to previous years, and well supported.	There is a sense of a limited awareness of the actor's description of his preparedness in relation to CS, based on the training received. The scope of this training seems to be very basic, based on anecdotal evidence.
	Kendall	DES: Actor - Confident in awareness; no clear process for vulnerability reporting; presented as intuitive, informal contact.	Again, the confidence of the actor in his ability to detect vulnerabilities is not underpinned by a familiarity with a procedure, distinct training or awareness of CS structures and procedures. Nor is it supported by previous experiences of the kind.

	Brooklyn*	DES: [SECTOR BODY] report highlights sector level sentiment; Universities seem more aware of the threats, with more dedicated security staff, better questionnaire response, and less satisfied, on average than Colleges. ["Could be from a position of ignorance"]. Posture depends on member of staff [technical vs. managerial]; Attitude non-homogenous, largely dependent on attack history	The link between awareness and self-evaluation is pretty evident in the data as well; Kendall/AN's confidence in their ability to identify threats is not justified by any visible capability on this specific task. Managerial posturing also apparent in data collection.
	Remy	DES: Large organisation - depends on process; Own devices mean user behaviour outside of procedural control and monitoring	Very technical view, associating scale with process and training/education.
	Sage	DES: in training, staff interested in technological safety and procedure; AN: More technical training and awareness is required	

	Rudy	DES: Policies are not known to everyone; AN: 'No one wants to be involved in a breach' DES: people 'very busy' - ' security isn't top of mind'; DES: Very hard to instil a culture of security	Procedural opaqueness seems to be a reoccurring theme. Pockets of knowledge and awareness prevent more effective user defensive behaviour, and also bypass IT and IS FUNCTION 'radars'
	Alex	DES: Communication amongst functions is essential; 'must speak business-speak'; 'must translate risk into business risk'	
	Fin	DES: Expectation of inherent safety with available platforms. Seemingly more aware than other actors of awareness limitations. Delegated liability for most selection to the institution. No familiarity with any mechanism of addressing vulnerabilities	Justifies concerns over education/transparency for this segment. The one way nature of the interaction between IS FUNCTION/IT and users is problematic as it relies on anticipation, audits and detection rather than staff feedback based on awareness of a given organisational context.
	Ash	DES: 'sub-system' dependence on individual capabilities, making turnover problematic; non-standardized nature of the capabilities is evident	

	Ash 2	DES: Importance of informal feedback networks to maximise awareness;	

Notes: Policies not known to everyone. High value of feedback obtained through informal means; 'ICT Risk' must be translated to business speak; Breaches occur in spite of intent, not because of it; Anecdotal evidence of staff interest in technological safety (Sage); Organisational size means that 'it —communication — depends on process'; Asymmetry in staff capabilities (ENT) and awareness; Posture depends on member of staff (technical or managerial); Actor awareness and self-evaluation ability seem limited; Limited threat awareness - bottleneck; Education deficit perceived