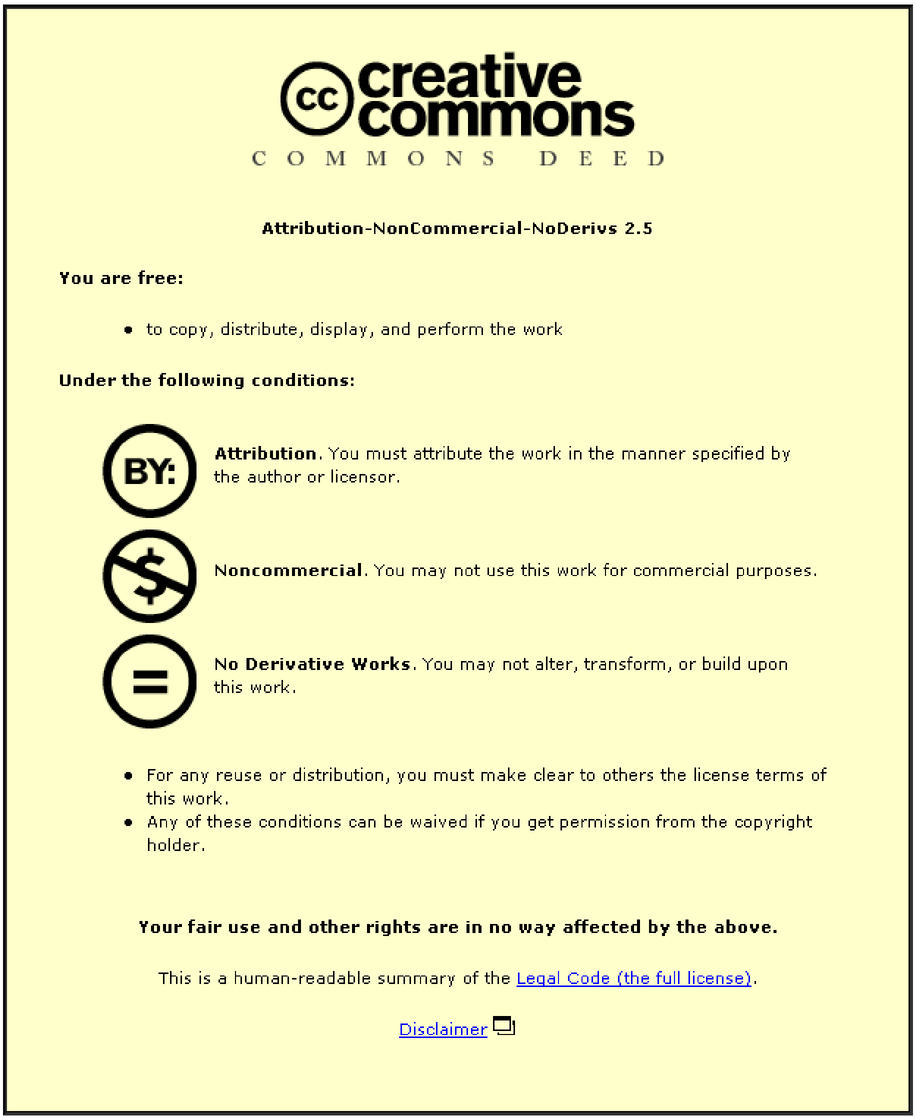

Reinforcing the security of corporate information resources: a critical review of the role of the acceptable use policy

Prof Neil Francis **Doherty**[a,]; Dr Leonidas **Anastasakis**[a]; Dr Heather **Fulford**[b]

[a] Loughborough University, The Business School, Ashby Rd, Loughborough, Leicestershire LE11 3TU, United Kingdom

[b] Aberdeen Business School, The Robert Gordon University, Garthdee Road, Aberdeen AB10 7QE, United Kingdom

Key Words: *Acceptable Use Policies; Computer Use Policies; Policy Positioning; Policy Content; Higher Education Sector*

Abstract: *Increasingly users are seen as the weak link in the chain, when it comes to the security of corporate information. Should the users of computer systems act in any inappropriate or insecure manner, then they may put their employers in danger of financial losses, information degradation or litigation, and themselves in danger of dismissal or prosecution. This is a particularly important concern for knowledge-intensive organisations, such as Universities, as the effective conduct of their core teaching and research activities is becoming ever more reliant on the availability, integrity and accuracy of computer-based information resources. One increasingly important mechanism for reducing the occurrence of inappropriate behaviours, and in so doing, protecting corporate information, is through the formulation and application of a formal 'acceptable use policy (AUP). Whilst the AUP has attracted some academic interest, it has tended to be prescriptive and overly focussed on the role of the Internet, and there is relatively little empirical material that explicitly addresses the purpose, positioning or content of real acceptable use policies. The broad aim of the study, reported in this paper, is to fill this gap in the literature by critically examining the structure and composition of a sample of authentic policies – taken from the higher education sector - rather than simply making general prescriptions about what they ought to contain. There are two important conclusions to be drawn from this study: 1) the primary role of the AUP appears to be as a mechanism for dealing with unacceptable behaviour, rather than proactively promoting desirable and effective security behaviours, and 2) the wide variation found in the coverage and positioning of the reviewed policies is unlikely to be fostering a coherent approach to security management, across the higher education sector.*

1 Introduction

All forms of modern organisation, whether they are operating in the public or the private sector, have become far more dependent upon a wide range of information technologies to support all aspects of their strategic and operational activities. Although such technologies may have the potential to deliver many important benefits, in practice, their contribution is often comprised, because of the unacceptably high levels of security breaches experienced [Garg et al, 2003; Whitman, 2004]. Ensuring the security of corporate information, that is increasingly stored, processed and disseminated using information and communications technologies [ICTs], has therefore become an extremely complex and challenging activity [Doherty et al, 2009]. Whilst many security problems can be attributed to the activities of external agencies and events, there is growing evidence that a high proportion of security problems are the result of errors, oversights or malpractices perpetrated by an organisation's own employees [Stanton et al, 2005]. Indeed, it has been noted that growing numbers of employers have had to discipline their own employees because they have breached organisational security policies and protocols [Stephen & Petropoulakis, 2007]. Breaches of information security range from the intentional acts of malicious behaviour through to naïve mistakes [Stanton et al, 2005], and cover issues such as: sharing passwords; forgetting to take back-ups; leaving PCs unattended; sharing sensitive information with outside parties, etc. [Leach, 2003].

One obvious response to the increasing variety of security threats to the effective use of corporate IT [Dhillon & Backhouse, 1996; Patel et al, 2008] is to implement a portfolio of the many technological fixes and defences, such as firewalls, patches, antivirus and content filtering software, that are now available [Ng et al, 2009; Herath & Rao, 2009a; Rhee et al, 2009]. Although such sophisticated technical tools, may play an important role in improving information security, particularly with respect to protecting an organisation from external threats, they are less well suited to detecting naïve, negligent or destructive employee behaviours [Ng et al, 2009]. Indeed, it can be argued that most organisational conceptualisations of information security are far too techno-centric [Dhillon & Torkzadeh, 2006], and that they typically ignore more socio-organizational issues such as trust, ethicality and the integrity of employees [Dhillon & Backhouse, 2000]. This may be a potentially dangerous oversight, because, no matter how sophisticated an organisation's technical defences, its information security '*ultimately depends on end user behaviour*' [Rhee et al, 2009: p. 2].

For the majority of organisations, the most obvious and appropriate strategy to control the behaviour of their computer users, is by introducing and enforcing an acceptable use [or 'usage'] policy [Foltz et al, 2008]. Such policies have been defined as the set of rules that are formulated, typically by senior IT managers, to clearly and explicitly define how all organizational computing resources may, or may not, be used by employees [Nolan, 2005]. Such policies are now extremely widely used, but they have, as yet, attracted very little explicit attention in the academic literature. Moreover, in the small number of instances in which the AUP has been the subject of academic research, the studies have tended to restrict their focus to Internet or telecommunications usage only [Lichtenstein & Swatman, 1997; Whitman et al, 1999; Siau et al, 2002].

Against this backdrop, the broad aim of the study, reported in this paper, is to help fill the significant gap in the literature with regard to the purpose, content and positioning of actual acceptable use policies, by empirically addressing the following research question: To what extent is a sample of genuine, and currently operational, AUPs effectively fulfilling their primary purpose, that is to clearly articulate to users how all organizational computing resources may, or may not, be used? More specifically, we wanted to both explore the extent to which best practice was being followed, in the areas in which it already exists, and to develop new insights, with regard to the many facets of AUP design that have as yet not been the subject of academic scrutiny. In particular, we were keen to investigate the extent to which best practice was being followed in terms of the purpose and content of the AUP, and the extent to which best practice could be established with respect to the positioning of such policies. In terms of the arena in which this study might best be conducted, we chose to focus on universities, because as knowledge-intensive organizations, the quality and security of their information assets should be a very high priority, for all organisations, right across the sector [Mok, 2005]. The remainder of this paper is organized into the following five sections: a review of the literature and a description of the research objectives; a discussion of the research methods employed; a presentation of the findings; a discussion of their importance and finally the conclusions and recommendations for future research.

2 Contextual Background

The aims of this section are threefold. Firstly we seek to review the literature, with regard to the justification for adopting an acceptable use policy, in terms of its stated purpose and objectives. Secondly, we investigate the extent to which the content of such policies has been addressed in the literature. Finally, the literature is summarised and critiqued, the gaps in it are identified, and the study's specific objectives articulated. Although for the purposes of this paper we have chosen to use the term '*acceptable use policy*', as it appears to be the most commonly used, it should be noted that in some organisations and literatures, other terms are used to describe the very same type of document. Consequently, this literature review has also targeted contributions that address '*Acceptable Usage Policies*' [Stephen & Petropoulakis, 2007], '*Computer Use Policies*' [Scott & Voss, 1994]; '*End-user Policies'* [Herath & Rao, 2009b] and '*Computer Usage Policies*' [Foltz et al, 2008], as their purpose and content is wholly relevant to the objectives of this study. Moreover, some other types of policy have also been included in this review – e.g. the '*Internet Acceptable Use Policy*' [Lichtenstein, 1996; Stewart, 2000] and the '*Telecommunications Policy*' [Whitman et al, 1999] – as even though they are restricted in their focus, they are very similar in terms of their broad purpose.

2.1 The Objectives of the AUP

When it comes to enforcing the security of organisational information resources, users are increasingly seen as the weakest link in the chain [Schneier, 2000]. Indeed, many organisations now view internal security threats to be a far more pressing issue, than external threats, such as hackers, viruses or natural disasters [Leach, 2003]. As the internal threat is often the result of poor security practices, on the part of the user, it can be argued that increasing user awareness, particular with regard to what behaviours are acceptable and unacceptable, should greatly help to nullify the internal threat [Siponen, 2000]. Against this backdrop, the acceptable use policy has been promoted as an organisation's key defence against the internal threat.

Although the Internet provides organisations with numerous business benefits, Anandarajan [2002] argues persuasively that it also provides employees with access to the world's '*largest playground*', in which they can waste time gambling, shopping, chatting, or simply browsing. Although the Internet is the most obvious computer resource upon which employees might waste time by engaging in '*cyber-loafing*' [Lim, 2002], it is not the only one, as unproductive behaviours, such as game playing, can also be witnessed on the stand-alone PC [Everton et al, 2005]. However, it has been argued that not all forms of '*cyber-loafing*' are intrinsically harmful to the host organisation, particularly if they help reduce employee stress and burnout [Lim & Chen, 2009]. Consequently, a key aim of the AUP is to clearly articulate, to users, which behaviours are deemed to be appropriate and what is inappropriate behaviour, with respect to their use of corporate IT resources [Attaran, 2000].

Many very serious external threats such as Trojans, hackers, worms or viruses [Huang et al, 2008] can be facilitated through naïve or sloppy user behaviour, such as poor choice of passwords, sharing passwords [Stanton et al, 2005] or the injudicious clicking on web links or opening of attachments in emails from unknown senders [Ng et al, 2009]. Consequently, in addition to clarifying the organisation's position with regard to the use of its computers, Nolan [2005] suggests that the AUP should also aim to minimise security threats, by promoting user awareness and good security practices. In most countries, organisations also have a legal obligation to take all reasonable steps to ensure that their employees can work in an environment that is free from all forms of harassment and discrimination [Salter & Bryden, 2009]. Unfortunately, there is significant evidence to suggest that many employees have been tempted to behave inappropriately or illegally, in their use of information systems. For example, in cases in which employees have been found to have used corporate information technologies to harass, discriminate, defame, act obscenely or breach copyright, then legal cases have successfully been brought against the employer [Herath and Wijayanayake, 2009]. Consequently, Scott [1997] highlights the important role that the AUP should also play in minimising the threat of litigation that organisations face, by making it clear to employees exactly what type of behaviours are absolutely unacceptable, because they might result in a costly law suit.

Not only is it important that the AUP fulfils each of this broad roles and objectives, it is essential that the policy document starts with a clear articulation of its specific purpose [Kilman & Stamp, 2005]. Moreover, best practice suggests that the policy's stated objectives should be tailored to the organisational context in which it will be utilised, so that it is explicitly aligned with the host organisation's strategies, goals and culture, as well as the specific risks that it is likely to face [Kilman & Stamp, 2005; Palmer et al, 2001; Stewart, 2000].

2.2 The Content of the AUP

A search of the Internet suggests that there is already a very significant body of advice, and established best practice, with regard to the '*ideal*' content / structure of the acceptable [or computer] usage policy, in the professional arena and on the Internet. However, this subject has attracted far less attention, to date, in the academic literature. In one of the very few papers to explicitly address this topic, Holmes [2003] suggests that the computer use policy should address the following seven issues:

i. monitoring use of proprietary assets;
ii. establishing no expectation of privacy;
iii. improper employee use;
iv. allowable employee uses,
v. protecting sensitive company information;
vi. disciplinary action,
vii. employee acknowledgement of policy

Whilst the above list is one of the very few attempts to articulate, in broad terms, the contents of the acceptable use policy, researchers have been more forthcoming in trying to define the contents of the '*Internet Acceptable Use Policy*'. For example, Lichtenstein [1996] identified a range of issues that should be included in such a policy, and grouped these into legal, managerial, administrative, operational, technical and human issues. In a similar vein, Lichtenstein & Swatman [1997] identifies some of the broad areas that it should cover, including: '*acceptable and unacceptable Internet uses*'; '*the roles and responsibilities of Internet users*', and '*the sanctions for non-compliance with the policy*'. In one of the very few empirical studies, in this domain, Siau et al [2002] investigated the contents of the '*Internet Acceptable Use Policy*', but only in terms of the abuses that were explicitly covered in a sample of policy documents. It was found that general email abuse, unauthorised usage and access and copyright abuses were the most commonly occurring issues covered by the Internet AUP. In the only other piece of empirical research, that we could find in this area, Whitman et al [1999] explored the content of '*telecommunications-use policies*'. They found that '*statements of policy*', '*authorized access and usage of equipment*', and '*prohibited usage of equipment*' were the most cost commonly covered issues, in their sample of policies.

2.3 Critique of literature and research objectives

Because of its increasingly important role in protecting organisations, and their employees, from costly mistakes, criminal activity and legal liability, the acceptable use policy is increasingly seen as one of the modern organisation's most important codes of practice [Foltz et al., 2008; Holmes, 2003; Lichtenstein,1996]. However, in comparison with the long-standing and extensive stream of literature addressing other forms of information security documentation, and in particular the information security policy [e.g. Straub & Welke, 1998; Rees et al, 2003; Doherty & Fulford, 2005], the literature that explicitly addresses the AUP is still rather immature. Consequently, despite its organisational importance, its purpose, structure and content have not, as yet, been subjected to a great deal of empirical scrutiny, in the academic literature. Indeed, even where the AUP has been empirically investigated, the studies have tended to be rather limited in their scope, restricting their focus to either Internet acceptable use policies [Siau et al, 2002] or telecommunications-use policies [Whitman et al, 1999]. Moreover, the existing studies of the acceptable use policy have tended to conceptualise it as a stand-alone document [e.g. Lichenstein, 1996; Siau et al, 2002], rather than explicitly addressing its relationship to the many other security documents, that, in their totality, are designed to protect and secure an organisation's information resources. Finally, and perhaps most importantly, given the rapid rate of change in organisational IT practices, there is a need for more up to date contributions, which reflect current concerns and behaviours.

Against this backdrop, the broad aim of the study, reported in this paper, was to critically examine the following three questions with respect to the design and positioning of acceptable use policies, as currently being used by some of the world's leading Higher Education Institutions [HEIs]:

i. What are the objectives of the acceptable use policies, as explicitly stated within the policy document?

ii. What specific issues and topics do acceptable use policies explicitly cover?

iii. How are acceptable use policies positioned, in terms of their explicit relationships with other information security documents?

It was envisaged that in addressing these questions a number important new contributions would be made to the literature. In particular it would help to establish the extent to which the stated purpose, the coverage and the positioning of AUPs was helping to promote acceptable behaviours, whilst restricting the incidence of unacceptable activities. Moreover, it would provide important new insights into how the purpose, coverage and positioning of genuine AUPs differ from the theory, as prescribed in the literature. It was also anticipated, that in empirically investigating the design of current policies, many important new issues and insights would be generated, that have, as yet, not been addressed in the extant literature.

3 Research Design and Methods

As our overarching aim was to understand the purpose, content and positioning of acceptable use policies, it made sense to critically examine actual policy documents, so that each could be processed and inspected in exactly the same way. To this end, we ultimately chose to focus our study on the AUPs of higher education institutions, as by and large, universities have been prepared to publish their core IT policies on their Internet sites. More specifically, our sampling frame consisted of the top 100 universities from the World University Rankings 2008 produced by the Time Higher Education Supplement (THES, 2008). It was envisaged that the world's leading universities, being at the leading edge of both academic and research activities, would also be at the frontier of effective information protection practices, via a coherent information security management programme. Furthermore, the use of THES rankings enabled us to target influential universities from a range of countries. However, given the difficulties of reviewing policies that weren't written in the native tongue of the research team, the sample was restricted to universities, based within English-speaking countries. The focus on English-speaking universities was not only governed by language considerations, but was also justified because countries such as USA, United Kingdom and Australia, amongst other English-speaking countries, dominate the rankings. More specifically, a total of 70 English-speaking universities were identified in the World's top 100 universities, which were based in a variety of countries, namely: USA, United Kingdom, Australia, Canada, Hong Kong, New Zealand and Ireland. Table 1 provides a break-down of this sample, in terms of the proportion from each country that make their AUP documents available, via their website.

Table 1: Breakdown of Sample

Country	No. of Universities in top 100 ranking	No. of policies available online	Percentage per country
USA	37	32	86.5
UK	17	17	100
Australia	7	7	100
Canada	4	4	100
Hong Kong	3	3	100
New Zealand	1	1	100
Ireland	1	1	100
TOTAL	**70**	**65**	**93%**

In order to ensure that the process of data collection from each reviewed 'acceptable use policy' was consistent and accurate a pro-forma was devised. Each AUP was reviewed by one of the investigators and subsequently cross checked by another. The pro-forma comprises four main sections: university details, policy objectives, policy coverage and links to supplementary security documents. The first section contains the name, country, position in worldwide university ranking of the university together with the URL address where the reviewed AUP can be found. In the policy objectives section we recorded the stated aims of the policy, whilst the policy coverage section was used to record the specific policy areas covered by the university's AUP. Finally, the fourth section was used to record details of any ancillary or supplementary policies, regulations and codes of practice that were also publically available on the universities' web-sites.

To ensure that the task of evaluating the content of policy documentation was conducted consistently, we created a classification of common policy issues that should be addressed in an AUP. In contrast to the information security policy [ISO, 2005], there is no common standard governing the design of AUPs. Consequently, a variety of other sources, ranging from academic journals [e.g. Lichtenstein, 1996; Lichtenstein & Swatman, 1997; Whitman et al, 1999; Siau et al, 2002] to information security websites[1], were consulted to derive a list of those issues that should be covered in an acceptable use policy. Ultimately, eight distinct policy areas of best practice were identified, resulting in the AUP framework described in table 2. These eight distinct issues were ultimately chosen because given their recognised importance and generic nature, they might be considered to comprise the minimum requirements for any well designed AUP document. However, as our primary aim was to provide a thorough overview of the coverage of universities acceptable use policies, the proposed AUP framework was only designed to serve as a point of departure for our research. Consequently, when reviewing our sample of AUPs, whenever a distinct new area of policy coverage was identified, it was given a new code, together with a brief description, and added to our framework, so that we could ultimately build a more complete picture of policy coverage. As will be demonstrated, in the next section, many of the reviewed policies ultimately covered a far wider range of distinct policy areas, than those minimum requirements, as presented in table 2.

Table 2: AUP Framework – Policy Coverage Areas

Policy Area	Description
Access Management	Covers issues such as who is authorised to use systems and corporate information; username and password management regulations and good practice guidelines
Acceptable Behaviour	Covers permitted user activities, such as work-related use of the systems and information, and internet usage in particular. Acceptable usage of email
Unacceptable Behaviour	Covers prohibited user activities, such as hacking, downloading illegal material, accessing illegal websites, dissemination of illegal or offensive material, sending bulk emails, harassment of other users, violating privacy of others users, dissemination of viruses, use of systems and/or corporate information commercial purposes, personal usage of systems and/or corporate information
Licence Compliance	Rules and regulations about software downloading, sharing and usage
Roles and Responsibilities	Explanation of the specific roles and responsibilities of users, system administrators, managers, and so on.
User Monitoring	Explanation of the organisation's approach to monitoring of user activities (e.g. email monitoring)
Sanctions for Policy Violations	Explanation of the actions that will be taken in the event of a user breaching the Acceptable Use Policy
Policy Management	Details of responsibilities and procedures for policy management and maintenance

4 Research Findings

The task of identifying a university's AUP document was not always straightforward, due to the very significant variations in the terminology used. Consequently, very large numbers of

[1] Influential not-for-profit organisations: **Becta** a British government agency leading the national drive to ensure the effective and innovative use of technology throughout learning; the **London Advice Services Alliance (LASA)** a charity providing ICT advice, consultancy and easy to read resources to the voluntary and community services; **Joint Information Systems Committee (JISC)** for the UK Further and Higher Education Funding Councils; The **SANS (SystemAdmin, Audit, Network, Security) Institute**, which is a cooperative research and education organization, specialising in information security.

on-line security documents often had to be reviewed in order to determine which one primarily addressed the acceptable use of information resources. The challenge of tracking down the AUP was exacerbated because the documents were not always stored in obvious, or easy to access, locations, on university web-sites. Ultimately, 65 policies were found and critically reviewed, and the key features of their objectives, structure and content are discussed below.

4.1 Objectives of the AUP

Having successfully isolated the policy document that addressed the '*acceptable usage of IT resouces*', the introductory statements in each policy were a useful means of revealing a university's broad outlook with regard to the acceptable use of its systems. It is reassuring to report that best practice is clearly being followed with regard to the requirement to clearly state the policy's purpose [Kilman & Stamp, 2005], as all the reviewed policies contained an explicit articulation of their objectives. Whilst there was some variation in stated objectives of the reviewed policies, there was a very high degree of commonality, and the following is a highly representative example:

> *The purpose of this policy is to deliver an information technology infrastructure that effectively supports the basic missions of the university in teaching, research and administration. In particular this policy aims to promote the following goals:*
>
> *i. to ensure the integrity, reliability, availability, and superior performance of IT systems;*
>
> *ii. to ensure that use of IT systems is consistent with the principles and values that govern the use of other University facilities and services;*
>
> *iii. to ensure that IT systems are used for their intended purposes;*
>
> *iv. to establish processes for addressing policy violations and sanctions for violators.*

This statement is important in a number of key respects. It clearly shows that the policy relates to an institution's complete IT infrastructure, and not just its Internet and networked resources; it reinforces the point that the policy should reflect both intended and unacceptable behaviours, and perhaps most importantly, it indicates that the policy should ultimately be focussed towards improving the performance of the institution's IT systems. An important area in which there was very little evidence that policies' were conforming to best practice relates to the need to tailor them to take account of organisational objectives and risks [Stewart, 2000; Palmer et al, 2001]. Policy objectives were typically stated in a fairly generic and predictable manner, with very little indication of any contextual tailoring. Although there was a relatively high degree of consistency, in terms of stated objectives of the reviewed policies, there was a far higher degree of variation with regard to the policies' positioning arrangements and coverage, but still no clear evidence of tailoring, as discussed in more detail in the remainder of this section.

4.2 Positioning of the AUP

To facilitate the acceptable use of organisational IT, the AUP must be well positioned both in terms of its naming and its relationship to other forms of security documentation, so that acceptable usage guidance is comprehensive and easily accessible. Indeed, in terms of the naming of these policies, there was evidence of a very high degree of variation. As can be seen from the results presented in table 3, whilst the '*Acceptable Use Policy*' is by far the most commonly used name, there are still eight other alternative titles, which have been adopted, amongst our sample of universities. This may not be a problem to the many users who will only be aware of the existence of this policy because their employers have explicitly drawn it to their attention. However, as higher education is a highly dynamic and increasingly multicultural sector, it is now common for researchers and academics to move between institutions, and even between countries, on a fairly frequent basis. Consequently, it would be helpful if a common terminology were adopted, so that individual employees can become acclimatised to the fact that it is an institution's AUP that sets the standard for their computing behaviours. Moreover, if the appellation '*Acceptable Use Policy*' were to become more commonly used across all institutions, operating within the global Higher education sector, then it would help to promote the AUP brand, and underline its importance. The other important insight to be gleaned from table 3, is that although the vast majority of the sample of universities studied [93%] had some form of documentation that was clearly and explicitly focused upon promoting the '*acceptable use*' of information resources, the adoption of this particular policy document is by no means universal.

In terms of its positioning, with respect to other forms of security documentation, it becomes clear that the AUP is but one of a growing portfolio of policies / guidelines, and procedures (see table 4). In addition to their primary policy on the '*accepted use*' of computing and information resources, the surveyed Universities have a number of ancillary policies, which are then further supplemented by tailored guidelines and/or procedures. Herein lies a major problem for both systems professionals and users, working within the university sector, as the majority of these ancillary policies and guidelines are not explicitly referenced from the acceptable use policy. Consequently, should a user wish to find guidance on their institution's stance on email or copyright infringement, there may well be significant confusion as to the which document[s] should be referenced. The existing literature recognises the need for organisations to develop an explicit framework of security policies, which clearly demonstrates the relationship between security policies and other security related documentation, such as standards, guidelines and procedures [Palmer et al, 2001; Kilman & Stamp, 2005]. The results of our study indicate that whilst frameworks of security documentation are evolving within the HE sector, they are by no means explicit and obvious to the user of such documentation. Consequently, these findings have important implications for best practice in that they highlight the need for all organisations to ensure that their policies, standards and procedures are explicitly cross referenced to all related security documents.

Table 3: Country breakdown and Naming of AUP and AUP-related documentation

Policy Title	USA	UK	Australia	Canada	Hong Kong	New Zealand	Ireland	Total
Acceptable Use Policy	24	2	4	2	2	1	0	35
Info. Tech. Policy	2	0	0	0	0	0	0	2
Code of Conduct	0	1	0	1	0	0	1	3
AU / IT Guidelines	1	0	1	0	0	0	0	2
AU / IT Regulations	0	10	1	0	0	0	0	11
AU / IT Rules	0	1	1	0	0	0	0	2
Conditions of Use	2	3	0	1	0	0	0	6
Ethics Policy	2	0	0	0	1	0	0	3
Info Security Policy	1	0	0	0	0	0	0	1
No obvious AU Policy	5	0	0	0	0	0	0	5

Table 4: Ancillary IT Policies Breakdown per Country

Policy Type	USA	UK	Australia	Canada	Hong Kong	New Zealand	Ireland	Totals
Information Security	29	7	5	1	0	1	1	44
Email	19	8	6	2	0	1	1	37
Privacy	14	0	2	1	3	0	0	20
E-commerce	6	0	2	0	0	0	0	8
Copyright	16	3	2	1	0	0	0	22
Guidelines/Procedures	24	15	6	2	3	0	1	51
Standards	7	5	1	1	0	0	0	14
Data Protection	2	7	0	0	0	0	0	9
Procurement	1	0	0	1	0	0	1	3
Infrastructure	15	8	4	2	2	1	1	33
Web/Domain	18	3	5	1	1	0	1	29
Web Publishing	6	5	1	0	0	0	1	13
Others	27	14	7	3	3	1	1	56

4.3 Coverage of the AUP

The analysis of specific security management issues addressed in the universities' security documentation, only considered the institutions' core acceptable use policy, and therefore any supplementary policies / guidelines / procedures were not explicitly reviewed. Each acceptable use policy was thoroughly reviewed to determine its coverage of the key usage issues, as highlighted in table 2. In some cases, a policy might have referred a reader to a supplementary policy, in which case this was deemed to be explicit coverage as the reference point was from the core 'acceptable use' policy. Issues covered in separate policies or procedures, but not explicitly mentioned in the 'acceptable use' policy, were not deemed to constitute explicit coverage in our examination, as it can be argued that the AUP should be the point of departure for addressing all acceptable usage issues.

As can be seen from the results of the study presented in table 5, no one individual policy area was common to our complete sample of university policies. Whilst access management and sanctions for policy violations are covered in the majority of policies, most issues are covered in only about half of the policies reviewed. It is perhaps not surprising, or even concerning, that there is a certain amount of variability of the content, within the reviewed policies, as it might indicate that universities are tailoring their policies to their own specific organisational circumstances, rather than blindly following the prescriptions from the literature, as summarised in table 2. However, given these documents are primarily designed to communicate / promote acceptable behaviours, it is rather more disturbing that so few explicitly address acceptable behaviour, and by no means all policies highlight unacceptable behaviours. It is also interesting to note that whilst less than two-thirds of the sample [40/65] explicitly articulate unacceptable behaviours, the vast majority [56 / 65] specify the sanctions for unacceptable behaviours, even if the form of these undesirable actions isn't always stated. The remainder of this section briefly highlights some of the other more interesting insights to be gained from a review of these core issues.

In the relatively few policies in which '*acceptable use*' is explicitly addressed, it is typically done through broad generalisations, rather than clear examples. As a result they simply state that acceptable use is such use that supports the research, education, administrative and other functions of the university. They also typically emphasise the need for acceptable use to respect the value and intended use of human and electronic resources as well as respect intellectual property, data ownership and users rights to privacy and freedom from intimidation. Only one University provided clear examples of acceptable behaviour, highlighting practices such as: '*if you check your emails from another person's computer you should log off after finishing your activity and ensure that your password has not been saved on the computer*'. Whereas acceptable use was given fairly short shrift, unacceptable behaviour was generally addressed more fully. The most commonly highlighted unacceptable behaviours are: transmitting viruses or chain emails, viewing pornography, harassment, defamatory activities, vandalism of properties etc. Less common prohibitions included: political lobbying; the personal use of IT for commercial purposes; the use of resources for playing games; the accessing of date/match making sites, the unauthorised deletion of another person's news group posting. Against this backdrop, it can be argued that the AUP could play a far more explicit and proactive role in promoting desirable and effective security behaviours, rather than simply highlighting unacceptable behaviours.

Table 5: The coverage of Acceptable Use Policies

Core Issue	USA	UK	Austral-ia	Canada	Hong Kong	New Zealand	Ireland	Total
Access Management	21	14	6	3	3	1	1	49
Acceptable Behaviour	5	2	1	0	0	0	0	8
Unacceptable Behaviour	19	12	5	2	2	0	0	40
License Compliance	18	11	6	3	2	1	1	42
Roles and Responsibilities	14	9	5	0	2	0	0	30
User Monitoring	16	8	6	3	2	1	0	36
Sanctions for Policy Violations	25	17	6	3	3	1	1	56
Policy Management	19	3	6	2	0	1	0	32

The sections on monitoring tended to be written in very general terms, basically focusing on the university's right to monitor emails and data for security purposes, as well as in case of any investigation into policy violations. Most also stress that when credible evidence of illegal or otherwise impermissible activity is discovered, then appropriate action will be taken. A section on ‘*sanctions*’ is also very commonly found, but once again, its content tends to be very general and predictable. The clear majority of universities tend not to be explicit on what these sanctions might be, but prefer more general statements such as: ‘*individuals found to have violated this policy may be subject to penalties including temporary or permanent reduction or elimination of some or all IT privileges*’. In some cases, it is also stressed that policy violations can, depending on their seriousness, lead to dismissal from the university, and possibly criminal prosecution. Six universities also explicitly state the possibility of users having to reimburse any costs which may arise from the breaches of the policy. Only one policy could be found in which a clear hierarchy of sanctions was articulated, as follows:

> *‘Where a breach of the policy is established, but not referred to a law enforcement agency, one or more of the following penalties may be imposed on a person responsible for involved in the breach: (a) warning, (b) formal written warning, (c)restriction or termination of access to ICT resources, the summary suspension of such access and/or rights pending further actions, including disciplinary action, (d) the requirement to provide compensation for any improper use of, or damage to ICT, (e) disciplinary sanctions, which may include dismissal of an employee, termination of a contract or the suspension or expulsion of a student from a course of study.’*

Policy management is not always explicitly covered as a separate section, in the policy's main body, but its practice can often be inferred by reviewing the policies’ history. Most policies appear to have a two to three year review cycle, although there are quite a few that haven't been modified since their inception (which could be anything up to ten years ago). A few universities explicitly mention a review cycle, but it is not always clear that this process has been enacted. With regard to who is responsible for the issue, maintenance and approval of the policy it seems that the management of the policy is typically the responsibility of a Chief Information Officer, whereas overall approval for the policy rests with a higher level (e.g. Provost, President, Pro Vice Chancellor, etc)

In addition to the core issues addressed in an AUP, as summarised in table 5, it was also possible to identify other important areas of policy coverage, as presented in table 6. A high proportion of our sample made explicit reference to external laws and policies that a user should be aware of when using the host institutions' IT infrastructure. There was obviously a very strong national orientation, with regard to those laws most frequently referenced in the AUPs. For example, explicit mentions of the following laws were common in the policies of US universities: Federal Copyright Laws, Federal Wire Fraud Laws, Federal Computer Fraud and Abuse Law, and the Federal Child Pornography Law. By contrast, in the UK policies, the Data Protection Act, the Copyright, Design and Patterns Act, the Computer Misuse Act and the Pornography Law were the most commonly encountered Acts of Parliament.

Where the personal use of IT is explicitly covered in AUP, it is typically covered at a very general level, by highlighting that whilst a small amount of personal usage of IT resources may be permitted, it mustn't adversely interfere with an employee's work obligations. In a small number of cases, the personal use of IT is addressed more fully. For example one university policy states:

> '*Use of resources for personal purposes is not generally permitted unless such use is kept to a minimum. Such a minimal use is considered appropriate for the personal use of email, the Internet and other university resources. Limited personal use is defined as use which incurs minimal additional expense to the university, is infrequent and brief, does not interfere with the operations of the university and does not violate any university policy or state/federal legislation and regulation.*

This same policy also sought to justify its stance on personal usage, by providing explicit guidance to users on how much a variety of typical personal usage activities might cost the university. Another policy makes the important point that as it may be very difficult, in a university context, to distinguish between personal and professional use of information resources, the University will rely on its employees to act '*responsibly and judiciously*'.

Table 6: Extra Issues [specific sections] in the Acceptable Use Policies

Issue	**USA**	**UK**	**Austral-ia**	**Canada**	**Hong Kong**	**New Zealand**	**Ireland**	**Total**
Security	10	5	1	1	0	0	0	17
Email Regulations	8	4	2	0	1	0	1	16
Disclosure of Information	7	4	1	1	0	1	0	14
Inappropriate Material	4	5	4	3	1	0	1	18
Personal Use of IT	22	9	5	3	0	1	1	41
External Laws / Policies	21	12	5	2	2	1	1	44

Finally, whilst the sampled AUPs do cover a great deal of ground, we were rather surprised to find absolutely no mention of the following recent technologies / developments which might have been usefully addressed: social networking sites (Facebook, Twitter, Beebo etc); Skype and other Voice Over Internet Protocol (VOiP) applications, Internet TV (e.g. BBC iPlayer) or file sharing websites. Whilst this is a potentially worrying finding, it is not greatly surprising, given the relative infrequency with which Universities' review and update their acceptable use policies. Indeed, this paper makes a further important contribution by highlighting that too often, universities are failing to follow established best practice, which suggests that all security policies should be reviewed and revised at regular intervals [Palmer et al, 2001].

5. Discussion

The flexibility and power of modern information technologies, in general, and the Internet, in particular, pose all organisations with a very real dilemma [Nolan, 2005]. On the one hand, unfettered access to information resources can facilitate creative, constructive and ultimately productive behaviours. Unfortunately, on the other, unconstrained access to information technology can result in a variety of wasteful, inappropriate and even destructive behaviours [Stanton et al, 2009]. Consequently, there is a pressing need to strike a balance between the availability and the security of corporate information resources, and well designed security documentation has a vital role to play in this process [Doherty & Fulford, 2006]. Although the acceptable use policy has an increasingly important role to play in ensuring that all corporate information resources are used appropriately and productively [Nolan, 2005], it has not been the subject of a great deal of focused academic scrutiny.

Against this backdrop, this study makes some important new contributions, as it is more clearly focused, up to date, and comprehensive, than previous studies, in this area. Most importantly, it can be concluded that the wide diversity of disparate policies and standards in use is unlikely to foster a coherent approach to promoting acceptable user behaviours, either within specific organisations, or across the sector. The fact that a variety of important issues have been omitted from a large proportion of the reviewed policies is greatly worrying, as it suggests that many critical aspects of security management are being left to chance, rather than being proactively and responsibly managed. It can be legitimately argued that as the AUP should be tailored to fit its organisational context, variations in its content are only to be expected. However, we would counter that this variation should come within the content of each specific core issue [see table 2], rather than in the very presence of each of these issues. For example, we would expect all AUPs to explicitly address unacceptable behaviour, but we would expect that the discussion of these behaviours be tailored to the requirements of a specific organisational context. As well as finding gaps in the coverage of policies, we also identified some issues that have not been considered within previous studies of the content of the AUP. More specifically, email regulations, the disclosure of Information, and the personal use of IT are all issues that have been shown to be making a useful contribution within the AUP.

This study also makes a further important contribution by demonstrating that the AUP is just one document, amongst a growing proliferation of security standards, procedure, policies and laws, the majority of which are attempting to moderate or improve the users' utilisation of corporate information resources, in some specified way. This poses a significant problem for senior IT and security managers, how can they best position and design their AUP so that it provides a fairly comprehensive, yet accessible, source of general user information, whilst also integrating effectively with other security documents, so that less common or more sophisticated issues can also be addressed. A final important contribution of this paper lies in its clarification of the focus of the AUP. Most previous empirical studies have focussed purely upon organisation's Internet policies [Lichtenstein, 1996; Lichtenstein & Swatman, 1997; Siau et al, 2002], and have therefore missed those important elements of the AUP, that address the acceptable usage of information resources that are not accessed through the web. For example, issues such as licence compliance, copyright issues, password control, access management and privacy apply to all corporate information resources, not just those accessed via the Internet.

If, as was suggested earlier, the user really is the weakest link in the information security chain [Schneier, 2000], then it is important to reflect upon the AUP's role in reinforcing this link. On the face of it, it can be argued that the widespread adoption of the AUP suggests that institutions are attempting to provide users with the knowledge they need to proactively use and manage their information resources more effectively and securely. However, the strong emphasis on policy violations and sanctions, supported by lists of unacceptable user behaviours, and laws that mustn't be infringed, it might equally be inferred that the AUP's primary role is to provide the justification for disciplining employees, if it should be found that they have been infringed the policy. Indeed, we would argue that as in far too many cases the emphasis is on what users mustn't do, rather than on what than can and should do, it can be inferred that the AUP has been designed to protect the host institution, rather than proactively educating the user. This interpretation is supported by the work of Albrechtsen [2007], who concluded that too often users don't feel that they have the knowledge to play a proactive role in promoting effective and desirable security behaviours. Indeed, there may well be simple to articulate prescriptions with regard to issues, such as: the cautious use of e-mail; effective password etiquette; the reporting of unexpected situations and the handling of sensitive information [Albrechtsen, 2007], that could be easily and productively incorporated into the AUP. Consequently, it will be important for academic researchers and university managers, alike, to explore how the content and structure might best be modified so that it places more explicit emphasis on educating the user and promoting effective behaviour, whilst still performing its important role in providing a mechanism for dealing with unacceptable behaviours.

There are a number of other practical lessons to be gained from this study, which may help managers improve the information security climate within their organisations. Although there is a great deal of variability across this sample of policies, in terms of their content and structure, it is possible to detect some areas of commonalty in their phrasing and language. It is, therefore, important to question how these policies are being formulated. If they are being created by simply cutting and pasting chunks from policy *pro formas* or other organisation's policies, then it is unlikely that a great deal of thought is going into their formulation. Consequently, we would recommend that AUPs be created from first principles, to ensure that they are explicitly tailored to their organisation's specific requirements / circumstances. Moreover, the fact that policies are so infrequently updated, is worrying, and would suggest that organisations need to adopt a far more proactive approach to their review and maintenance. Finally, the proliferation of user-related security documentation suggests that organisations need to pay far more attention to managing it more holistically, to ensure that all security information is well integrated, and easy to find and assimilate. If security documentation is not readily accessible, then it can be easily subverted or ignored [Herath & Rao, 2009b], often with disastrous consequences.

Concluding Remarks

The work presented in this paper makes an important contribution to the information security literature as it presents one of the first, if not the first, objective, rigorous and independent evaluations of the positioning and content of authentic acceptable use policies, within a well-bounded organizational setting. In so doing, it highlights some worrying deficiencies in terms of the explicit coverage of policy issues and the ability of organizations to effectively cross-reference and integrate their portfolios of information security documentation. Research into the adoption of sophisticated policies, within a dynamic organizational context, is an ambitious undertaking, and therefore contains a number of inherent limitations. In particular, the adoption of the survey format restricts the range of issues and constructs that can be explored, and does not give the researcher the opportunity to explore why specific decisions, with respect to the structure and coverage of the policy, were taken. To this end, a series of follow-up interviews and focus groups are currently being planned, to help interpret and explain the results of our documentation review. In particular, we are keen to explore how the content of the policies reflects, and aligns with, the universities' strategic planning process. It will also be important to replicate this study in a variety of other sectors to test the generalisability of our findings. A further important aspect of our future research agenda will be to monitor how this sample of AUPs changes over a period of time, so that we can gain some insights both into the updating mechanisms for these policy documents, and also monitor the way in which security concerns are dynamically changing. Finally, although it may never be possible, or indeed beneficial, to try to include complete lists of acceptable behaviour in AUPs, future research might be usefully focused upon identifying and validating those specific user behaviours and best practice, that if enacted can deliver real improvements to organisational security. As the project unfolds, it is anticipated that the findings will help organizations to better understand the value of security policies and to pinpoint the policy areas for prioritisation.

References

Albrechtsen, E. (2007) “A qualitative study of users’ view on information security”, *Computers & Security*, **26** (4), 276-289.

Anandarajan, M. (2002) “Internet abuse in the workplace”, *Communications of the ACM,* **45** (1), 53–54.

Attaran, M. (2000) “Managing legal liability of the Net: a ten step guide for IT managers”, *Information Management & Computer Security,* **8** (2), 98-100.

Dhillon, G. & Backhouse, J. (1996) “Risks in the use of information technology within organisations”, *International Journal of Information Management*, **16** (1), 65-74.

Dhillon, G. & Backhouse, J. (2000) “Information System Security Management in the New Millennium”, *Communications of the ACM*, **43** (7), 125-128.

Dhillon, G. & Torkzadeh, G. (2006) “Value-Focused Assessment of Information System Security in Organizations”, *Information Systems Journal*, **16** (3), 293-314.

Doherty, N. F., Anastasakis, L. and Fulford, H. (2009) “The information security policy unpacked: a critical study of the content of university policies”, *International Journal of Information Management*, **29**(6), 449-457.

Doherty, N. F., and Fulford, H. (2006) “Aligning the information security policy with the strategic information systems plan”, *Computers & Security*, **25** (1), 55 – 63.

Doherty, N.F. & Fulford, H., (2005) "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis", *Information Resources Management Journal*, **18** (4), 21-38.

Everton, W. J., Mastrangelo, P. M. and Jolton, J. A. (2005) “Personality Correlates of Employees' Personal Use of Work Computers”, *CyberPsychology and Behavior,* **8** (2), 143-153.

Foltz, C. B., Schwager, P. H. and Anderson, J. E. (2008) “Why users (fail to) read computer usage policies”, *Industrial; Management & Data Systems*, 1**08** (6), 701-712.

Garg, A., Curtis, J. and Halper, H. (2003) “Quantifying the financial impact of information security breaches”, *Information Management and Computer Security*, **11** (2), 74-83.

Herath, T. and Rao, H. R. (2009a) “Protection motivation and deterrence: a framework for security policy compliance in organisations”, *European Journal of Information Systems*, **18** (2), 106–125.

Herath, T. and Rao, H. R. (2009b) “Encouraging information security behaviours in organizations: Role of penalties, pressures and perceived effectiveness”, *Decision Support Systems,* **47** (2), 154–165.

Herath, H. M. P. S. and Wijayanayake, W. M. J. I. (2009) “Computer misuse in the workplace”, *Journal of Business Continuity & Emergency Planning*, **3** (3), 259-270.

Holmes, J. (2003) “Formulating an effective computer use policy”, *Information Strategy: The Executive’s Journal*, **20** (1), 26-33.

Huang, D-L., Rau, P-L. P. Rau and Salvendy, G. (2008) “Perception of Information Security”, *Behaviour & Information Technology*, November, 1-12.

I.S.O. (2005) *Information technology – Security Techniques -. Code of practice for information security management - ISO 17799*. International Standards Organization, Geneva.

Kilman, D. and Stamp, J. (2005) “Framework for SCADA security policy”, *Technical report, Sandia Corporation*.

Lichtenstein, S. (1996) “Internet acceptable usage policy”, *Computer Audit Update*, **1996** (12), 10-20.

Lichtenstein, S. and Swatman, P. M. (1997) “Internet acceptable usage policy for organisations”, *Information Management & Computer Security*, **5** (5), 182-190.

Leach, J. (2003) “Improving user security behaviour”, *Computers & Security*, **22** (8), 685-692.

Lim, V. K. G. (2002) “The IT Way of Loafing on the Job: Cyberloafing, Neutralizing and Organizational Justice” *Journal of Organizational Behavior*, **23** (5), 675-694.

Lim, V. K. G. and Chen, D. J. Q.(2009) 'Cyberloafing at the workplace: gain or drain on work?', *Behaviour & Information Technology*, November, 1-11.

Mok, K. H. (2005) “Fostering entrepreneurship: Changing role of government and higher education governance in Hong Kong”, *Research Policy*, **34** (4), 537-554.

Ng, B-Y Kankanhalli, A. & Xu, Y. (2009) “Studying users' computer security behavior: A health belief perspective”, *Decision Support Systems,* **46** (4), 815–825.

Nolan, (2005) “Best practices for establishing an effective workplace policy for acceptable computer usage”, *Information Systems Control Journal*, **6**, 32-34.

Palmer, M. E., Robinson, C., Patilla, J. C. and Moser, E. P. (2001) “Information security policy framework: best practices for security policy in the e-commerce age”, *Information Security Journal: A Global Perspective*, **10** (2), 1-15.

Patel, S. C., Graham, J.H. and Ralston, P. A. (2008) “Qualitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements”, *International Journal of Information Management*, **28** (6), 483-491.

Rees, J., Bandyopadhyay, S. & Spafford, E. H. (2003) “PFIRES: A Policy Framework for Information Security”, *Communications of the ACM*, **46** (7), 101-106.

Rhee, H-S, Kim, C. & Ryu, Y.U. (2009) ‘Self-efficacy in information security: it’s influence on end-users information security practice behaviour’, *Computers & Security,* **28**, 816-826.

Salter, M. & Bryden, C. (2009) “I *can* see you: harassment and stalking on the Internet”, *Information & Communications Technology Law*, **18** (2) 99 - 122

Schneier, B (2000), *Secrets & lies*, *Digital security in a networked world*, John Wiley, New York.

Scott, T. J. and Voss, R. B. (1994) “Ethics and the 7 ‘Ps’ of Computer Use Policies”, in *Proceedings of the conference on Ethics in the computer age*, Kizza, J. M. (Ed), 61-67.

Scott, M. D. (1997) “Creating a corporate internet acceptable use policy”, *Computer Law & Security Report*, **13** (6), 451-453.

Siau, K., Nah, F. F., & Teng (2002) “Acceptable Internet use policy”, *Communications of the ACM*, Teng (2002) “Acceptable Internet use policy”, Communications of the ACM, **45** (1), 75-79.

Siponen, M. (2000) “A conceptual foundation for organisational information security awareness”, Information Management & Computer Security”, **8** (1), 31-41.

Stanton, J. M., Stam, K. R., Mastrangelo, P. & Jolton, J. (2005) “Analysis of end-user security behaviours”, *Computers & Security*, **24** (2), 124-133.

Stephen, B. & Petropoulakis, L. (2007) “The design and implementation of an agent-based framework for acceptable usage policy monitoring and enforcement”, *Journal of Network & Computer Applications,* **30**(2), 445-465.

Straub, D. W. & Welke R. J. (1998) “Coping with systems risk: Security planning models for management decision making”, *MIS Quarterly*, **22** (4), 441-470.

Stewart, F. (2000) “Internet Acceptable Use Policies: navigating the management, legal and technical issues, *Information Security Journal: A Global Perspective,* ***9*** *(3), 1 -7.*

THES (2008) 'World University Rankings', 2008. *The Times Higher Education Supplement*. Available at: http://www.timeshighereducation.co.uk/hybrid.asp?typeCode=243 (Accessed January 2009).

Whitman, M. E., Townsend, A. M. and Aalberts, R. J. (1999) “Considerations for an effective telecommunications-use policy”, *Communications of the ACM*, **42** (6), 101-108.

Whitman (2004) “In defense of the realm: understanding threats to information security”, *International Journal of Information Management*, **24** (1), 43-57.