International Journal of Information Management 29 (2009) 449–457

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

The information security policy unpacked: A critical study of the content of university policies

Neil Francis Doherty[a,*], Leonidas Anastasakis[a,1], Heather Fulford[b,2]

[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

ARTICLE INFO

Article history:

Keywords:
Information security policies
Security breaches
Policy content
Higher education sector

ABSTRACT

Ensuring the security of corporate information, that is increasingly stored, processed and disseminated using information and communications technologies [ICTs], has become an extremely complex and challenging activity. 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 security breaches, and in so doing, protecting corporate information, is through the formulation and application of a formal information security policy (InSPy). Whilst a great deal has now been written about the importance and role of the information security policy, and approaches to its formulation and dissemination, there is relatively little empirical material that explicitly addresses the structure or content of security 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 content of authentic information security policies, rather than simply making general prescriptions about what they ought to contain. Having established the structure and key features of the reviewed policies, the paper critically explores the underlying conceptualisation of information security embedded in the policies. There are two important conclusions to be drawn from this study: (1) the wide diversity of disparate policies and standards in use is unlikely to foster a coherent approach to security management; and (2) the range of specific issues explicitly covered in university policies is surprisingly low, and reflects a highly techno-centric view of information security management.

1. Introduction

It was over 20 years ago now that commentators, such as Porter and Millar (1985) and Drucker (1988), first recognised that an '*information revolution*' was taking place. This revolution had an immediate impact, and still has significant effects upon all aspects of organisational life (Zammuto, Griffith, Majchrzak, Dougherty, & Faraj, 2007). For example, not only do information and information technologies have the potential to deliver significant improvements in organisational performance (Brynjolfsson & Hitt, 1996; Sircar & Choi, 2007; Ward & Peppard, 2002), they can also dramatically reshape organisational processes, structures and cultures and the job specifications of individual employees (Doherty, King, & Al-Mushayt, 2003; Markus, 2004). Given its growing importance, information is often viewed as being analogous to an organisation's '*lifeblood*': should the flow of information become seriously restricted or compromised then the organisation may wither and die (Peppard, 2007). But it is not just information that caused an organisational stir, as in recent years the need to explicitly and proactively manage organisational knowledge has also been recognised (Johannessen & Olsen, 2003). However, the emergence of the knowledge-intensive organisation (KIO) (Sheehan & Stabell, 2007) should not be seen as being somehow distinct from the on-going information revolution, as both developments have only been made possible as a result of the dramatic improvements witnessed in the power, speed, flexibility and overall effectiveness of IT infrastructures (Desouza & Vanapalli, 2005; du Toit, 2003).

Although the modern enterprise is increasingly dependent upon high quality information, in practice, information resources are often incomplete or compromised, because of the unacceptably high levels of security breaches experienced (Garg, Curtis, & Halper, 2003). For example, in the UK, it has recently been found that '*the number of security incidents continues to rise*', with 74% of businesses reporting a security breach in 2004, as compared with only 44% in 2000 (DTI, 2004, p. 1). In a similar vein, Austin and Darby

* Corresponding author. Tel.: +44 1509 223128; fax: +44 1509 223960.
E-mail addresses: n.f.doherty@lboro.ac.uk (N.F. Doherty), L.Anastasakis@lboro.ac.uk (L. Anastasakis), h.fulford@rgu.ac.uk (H. Fulford).
[1] Tel.: +44 1509 223175; fax: +44 1509 223960.
[2] Tel.: +44 01224 263869.

0268-4012/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ijinfomgt.2009.05.003

(2003, p. 121) note that in the United States '*security breaches affect 90% of all businesses every year, and cost some $17 billion*'. Moreover, Austin and Darby (2003) also suggest that protective measures can be very expensive: '*the average company can easily spend 5% to 10% of its IT budget on security*'. One increasingly important mechanism for protecting corporate information, and in so doing helping to safeguard organisational knowledge assets, is through the formulation and application of a formal information security policy (Hinde, 2002; von Solms & von Solms, 2004). The broad consensus within the literature is that the information security is a high level document, which defines the organisations' goals, intentions and priorities, with respect to the management of information security, as well as highlighting the roles, rights and responsibilities of individual members of staff, with respect to the attainment of the security objectives (Hone & Eloff, 2002a; Hong, Chi, Chao, & Tang, 2006). Given their perceived importance, it is not surprising that there is already an established literature, with respect to the importance and role of the policy, as well as approaches to its formulation and dissemination. However, by contrast, there is very little published material that explicitly addresses the scope or content of security policies, in general, nor with respect to how they have been applied within specific organisational sectors, in particular.

Against this backdrop, the broad aim of the study, reported in this paper, is to fill this gap in the literature by empirically examining the content and structure of actual information security policies, rather than simply making prescriptions about what they ought to contain. More specifically, we chose to focus this study on universities, because as knowledge-intensive organisations, 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 twofold. Firstly we seek to use the literature to critically review the role of the information security policies in safeguarding the security of information assets before identifying the gaps in the literature and articulating the study's specific objectives.

2.1. The role and scope of the information security policy

There is a growing consensus within the literature that the information security policy is an increasingly important business document, which is uniquely well placed to proactively safeguard the availability, confidentiality and integrity of corporate information resources (e.g. Baskerville & Siponen, 2002; David, 2002). More specifically, it has been argued that this document should '*set out the organisation's approach to managing information security*' (ISO, 2005, p. 3). To this end, a good information security policy should:

> '*outline individual responsibilities, define authorized and unauthorized uses of the systems, provide venues for employee reporting of identified or suspected threats to the system, define penalties for violations, and provide a mechanism for updating the policy*' (Whitman, 2004, p. 52).

Perhaps the most critical role of the information security policy is to explicitly define the specific rights and responsibilities of individual users, and to communicate these successfully to each and every employee, so that a uniform, coherent and effective approach to information security is adopted across the organisation (Hone & Eloff, 2002b; Hong et al., 2006; Rees, Bandyopadhyay, & Spafford, 2003). Employees must have no excuse for not being able to apply defined security practices in accordance with the established policy (Saleh, Alrabiah, & Saad, 2007). Consequently, the policy must act as the point of departure for employees with respect to all information security issues, and in so doing, it becomes the '*heart and basis*' of successful security management (von Solms & von Solms, 2004, p. 374).

Whilst a substantial body of literature has evolved, and much consensus displayed, with regard to the role, importance and successful deployment of the policy, there has been rather less focus upon, and certainly far less unanimity with respect to, its content and coverage. The bulk of this literature has explored how the policy should be structured, typically from a conceptual perspective. For example, Baskerville and Siponen (2002) explore whether there should be a single policy, or if it should be subdivided into several distinct levels or types. Other scholars have also pondered the ideal structural arrangements with regard to the InSPy. Siponen (2000) suggests a two category model: '*computer-oriented* and *people/organisational policies*'. By contrast, Sterne (1991) favours a three level model, namely the '*institutional policy*, *the institutional ISP and the technical ISP*'. Finally, Lindup (1995) proposes four distinct levels: '*system security policy*, *product security policy*, *community security policy and corporate information security policy*'. Despite the continuing debate about the ideal number of policies, and how these might be inter-related, Lindup (1995, p. 691) notes that, in practice, organisations tend to have a single '*corporate*' information security policy. Other academics have focused upon the distinction between high level policies and the lower level practices that might usefully be produced, in support of the policy (Dhillon, 1997; Moule & Giavara, 1995), although it has been argued (Rees et al., 2003) that the policy should provide some guidance on '*means*' as well as '*ends*'. In more recent years, there has been a great deal less explicit focus, in the literature, on the most effective configuration for information security documentation, but certainly no resolution or consensus with respect to this issue. Indeed, the situation has been made rather more complicated through the growth of newer forms of security documentation – such as: '*Internet and email usage policies*' (Arnesen & Weis, 2007); '*copyright policies*' (Loggie et al., 2006); etc. – that might complement the information security policy. Consequently, there is a pressing need for focused, empirical research to explore the structural arrangements with respect to actual information security policies, as they are being currently applied in the organisational context.

In sharp contrast to the literature on the structure of the InSPy, which is plentiful but lacking in empirical contributions and consensus, the academic discussion of the specific issues that should be addressed by the InSPy is simply very sparse. The international standard 17799[3] (ISO, 2005) provides a useful indication of the types of issues that should be addressed, but these issues have been subjected to fairly limited academic scrutiny. One of the very few attempts to explicitly fill this gap was an empirical study of the use of the information security policies within large UK-based organisations (Fulford & Doherty, 2003), based upon a framework of potential policy issues synthesised from the literature. Whilst this study provides some very useful input into the debate, it was based upon the perceptions of IT managers about the content of their own policies, rather than an objective review of the actual content of policies, to ensure a consistency of approach and terminology.

[3] Please note that that the international standard that we used in the design of our study – ISO 17799 – has recently been re-badged as ISO/IEC 27002, but its content has in no way changed (Calder & Van Bom, 2006).

Table 1
A taxonomy of information security policy issues (after 3).

Issue	Description
Personal usage of information systems	The information security policy should clearly articulate the individual employee's rights and responsibilities in their use of organisational information systems.
Disclosure of information	Information systems increasingly allow employees direct access to significant amounts of information—much of which may be confidential. The security policy must therefore highlight any restrictions with regard to the disclosure or use of such information.
Physical security of infrastructure and information	Because of its high value, hardware and software are both potential targets for thieves. It is therefore important that the policy articulates strategies for the protection of infrastructure and information resources.
Violations and breaches of security	As security breaches are still a common and potentially damaging, occurrence, the policy document must indicate the steps to be taken to recover from a breach or violation and the requirements for recording such security incidents.
Prevention of viruses and worms	In response to the rapid proliferation of viruses, worms and trojans, the organisation's policy should be clear with regard to the application of virus checking software, the use of attachments and the sharing of information.
User access management	The information security policy should provide clear guidance on how access controls are to be allocated and managed, in line with business requirements.
Mobile computing	The use of notebooks, palmtops and laptops away from the traditional working environment makes them very vulnerable, as they are more difficult to protect using conventional security controls. The policy must therefore highlight the organisation's stance and practices with respect to secure mobile computing.
Internet access	As the corporate use of the Internet continues to grow rapidly, it is important that the policy explicitly addresses the issue of Internet access, particularly with respect to issues such as the viewing of pornography and personal browsing.
Software development and maintenance	As many security problems can be directly attributed to errors and oversights in the development of information systems, the policy must present guidelines for ensuring that effective security controls are built into all new systems.
Encryption	The growth of electronic commerce and mobile computing has greatly increased the amount of information that is being communicated across public – and potentially less secure – networks. The policy must therefore address the organisation's requirements for encrypting/protecting such information.
Contingency/continuity planning	It is essential that all organisations have a contingency plan in place to specify how to cope with and recover from a significant security breach, such as a natural disaster. The security policy must specify how such contingency plans are to be written, tested, maintained, and ultimately implemented.

Moreover, the Fulford and Doherty (2003) study focuses on the experiences of large organisations in general, rather than focusing specifically on the practices of organisations, within a specific sector, in particular. However, the Fulford and Doherty (2003) taxonomy does provide a very useful point of departure for the analysis of information security policies, in our study (see Table 1).

In addition to questions concerning the content and structure of the information security policy, there are also issues with respect to its effectiveness. The vast majority of organisations now claim to have formulated and implemented a formal information security policy (Fulford & Doherty, 2003; Hagen, Albrechtsen, & Hovden, 2008). Unfortunately, the persistently high incidence of security breaches (Dhillon, 2004; Kotulic & Clark, 2004; Straub & Welke, 1998) may suggest that the information security policy is not always delivering the goods (e.g. Hone & Eloff, 2002b; Karyda, Kiountouzis, & Kokolakis, 2005). Indeed, a recent study by Doherty and Fulford (2005) showed that in terms of the numbers of security breaches experienced, there was no significant difference between those organisations that had adopted an information security policy, when compared to those that had not. One potential explanation as to the apparent ineffectiveness of information security policies is that they adopt a very narrow definition of information security, which only focus upon issues of information confidentiality, integrity and availability (Dhillon & Backhouse, 2000). Unfortunately, such techno-centric conceptualisations of information security fail to address its increasingly important people and organisational dimensions (Dhillon & Torkzadeh, 2006). Indeed, support for this hypothesis is provided by the technically oriented conceptualisation of information security (Siponen, 2005) which is embedded in the most commonly adopted policy standard, the international standard 17799 (ISO, 2005): it explicitly focuses upon issues such as the availability, confidentiality and integrity of data, but ignores more socio-organisational issues such as trust, ethicality and the integrity of employees (Dhillon & Backhouse, 2000).

2.2. Summary and research objectives

Because of its increasingly critical role in preventing, detecting and responding to security breaches, the information security policy is widely acknowledged to be the single most important information security mechanism (von Solms & von Solms, 2004; Wadlow, 2000; Whitman, 2004), and should therefore have a particularly important role to play in the modern IT-enabled organisation. However, there are a number of key gaps in the literature, particularly with regard to the scope and content of authentic information security policies that make its suitability, in this role, difficult to judge. Consequently, the aim of the study, reported in this paper, is to explicitly address the gaps in the literature by exploring the following two research objectives:

1. To critically analyse the overall structure of information security policies, particularly in terms of the number of policies in use and how these relate to each other, and to related, lower level standards and procedures.
2. To investigate the variety of specific issues, as highlighted in Table 1, that are explicitly covered by information security policies.

When addressing these two primary objectives, we were also keen to consider the following two supplementary themes: do policy documents reflect a purely technical conceptualisation of information security management (Dhillon & Torkzadeh, 2006), and have these policies been specifically tailored to take account of their knowledge-intensive context?

Table 2
Breakdown of sample.

Country	No. of universities in top 200 ranking	No. of policies available online	Percentage per country
USA	57	26	46%
UK	32	18	56%
Australia	12	8	67%
Canada	11	6	55%
Hong Kong	4	1	25%
New Zealand	3	1	33%
Ireland	2	1	50%
South Africa	1	0	0%
Total	122	61	50%

3. Research design

It has been previously acknowledged that gathering of data from organisations, relating to the management of information security, may be difficult because of the sensitivity and confidentiality of the subject matter. As Kotulic and Clark (2004, p. 605) note, information security research is '*one of the most intrusive types of organisation research*' which leads organisations to mistrust the external researcher endeavouring to gather data about them. For this reason, and based on their negative experiences of research in the area, Kotulic and Clark (2004, p. 605) caution against the use of mail surveys for data gathering in information security research. In a similar vein, a recent DTI sponsored study of IT security (DTI, 2004, p. 4) also noted that its response rate had been significantly depressed because potential respondents had expressed concerns about the confidentiality and sensitivity of their contributions. Happily, in the present research, such data gathering problems could be avoided as our focus on policy analysis allowed us to gather the requisite data directly from the policy documents being used in organisations, rather than having to rely on individual informants within each organisation. More specifically, for the purposes of this study, we choose to target universities, as a very large proportion are prepared to disseminate their information security policy documentation by placing it on their web sites, thus making it available in the public domain. Our process of data gathering, therefore, entailed identifying a number of universities for investigation, consulting their web sites, and locating their information security policy documentation on those sites, ready for analysis.

The universities included in the study were selected from the World University Rankings 2007 produced by the Times Higher Education Supplement (THES, 2007). This ranking of the top 200 universities worldwide formed the sampling frame for the study, since it claimed to be based on five indicators chosen to '*reflect strength in teaching, research and international reputation, with the greatest influence exerted by those in the best position to judge: the academics*' (THES, 2007) Further, according to the THES (2007), the measures used create the ranking have been '*designed to be as objective as possible and as free as possible from international cultural bias*'. Those measures include peer review, citations per faculty member, faculty–student ratio, proportion of overseas students, and proportion of overseas faculty members. The use of this ranking for our study enabled us to target influential universities from a range of countries.

Having identified the ranking list of the top 200 universities, our approach was then to focus, in the first instance, on universities from English-speaking countries. The web site of each university from these countries was consulted in order to establish whether an information security policy was accessible via their site. In total, there were 122 English-speaking universities, in our sample, whose web sites could be easily reviewed to determine whether they had a policy document available online. Of this subset of 122 universities, 61 of these currently had a policy, which could be downloaded and evaluated. The policies examined are from universities in the following countries: United States of America, United Kingdom, Australia, Canada, New Zealand, Hong Kong, Ireland and South Africa. The table below (Table 2) shows the number of university sites consulted and the number of those universities making their information security policy available via their site.

When undertaking any empirical research, based upon a sample of a larger population, there is always a danger that the results and lessons learned may be diluted, or even undermined, through the introduction of bias (Churchill, 1997). In this study, it is possible to raise a number of questions with respect to the representativeness of our sample. For example, are universities representative of other large organisations? Are universities in the top 200, typical of other universities? Are English-speaking universities representative of the wider population? And finally, are policies posted on the Internet similar to those which remain subject to restricted access? Whilst it is not possible to totally exclude the possibility of bias, the fact that the chosen sampling frame is the planet's 200 most influential universities, and that we were able to thoroughly review the information security policies of over 30% of these, does suggest that the findings are likely to be important, and of interest to a wide variety of organisations and managers, both within and outside the confines of the sampling frame.

In order to ensure that the process of data collection from each information security policy was consistent and accurate, a *pro forma* was devised. To validate the research instrument employed, this *pro forma* was pre-tested in a pilot study during which the policies of ten universities were reviewed. As a result of this pilot, some minor refinements were made to the *pro forma*, and the study was then conducted. The *pro forma* data collection document comprised the following four broad components:

1. *University details*: name, country, position in worldwide university ranking, web site address.
2. *Policy structure*: details of which types of policy were available via the site, other than the information security policy. Such policies included acceptable use policy, electronic commerce policy, electronic mail policy, and privacy policy. The range of additional procedures or guidelines in place was also recorded.
3. *Policy administration details*: details about the date the information security policy was created, date of the last update, person/department responsible for the creation of the policy, and the person/department responsible for policy management and maintenance.
4. *Policy coverage*: based on the policy areas in the Fulford and Doherty (2003) taxonomy, the following policies areas were included on the *pro forma*: personal usage of information systems, disclosure of information, physical security, violations and breaches, viruses, system access control, mobile computing, Internet access, software development, encryption and contingency planning (see Table 1). Where explicit coverage of an area was noted in a policy, then the following additional details about the area were recorded: person/s responsible for the policy area; prohibitions in force relating to that area; the permissions

Table 3
Policies and guidelines/procedures.

Policy type	Total	Country breakdown						
	Universities	USA	UK	AUS	CA	HK	N.Z.	IRL
Information security policy	61	26	18	8	6	1	1	1
Acceptable use policy	52	20	17	8	4	1	1	1
Electronic mail policy	35	13	12	6	1	1	1	1
Copyright policy	17	7	6	3	1	0	0	0
Privacy policy	16	11	2	2	0	1	0	0
Data protection policy	11	9	0	1	1	0	0	0
Web publishing policy	7	2	3	3	0	0	0	1
Procurement policy	6	1	3	1	0	1	0	0
Web and domain names	6	5	4	0	0	0	1	0
E-commerce policy	3	3	0	0	0	0	0	0
Infrastructure policy	3	0	2	0	0	1	0	0
Freedom of information	1	1	0	0	0	0	0	0
Other guidelines/procedures	33	17	11	2	1	1	0	1

granted in relation to that area; and the penalties in place should the policy area be contravened. Additional fields were available within the *pro forma* for recording any other pertinent details about each policy area: we were particularly keen to identify any explicit references to security objectives or the security of knowledge.

Data were gathered by examining print outs of each policy in turn and completing the *pro forma*. This task was carried out by one of the investigators and subsequently cross-checked by a co-investigator to ensure accuracy and consistency. The contents of the *pro forma* were then summarised in tables to enable comparisons to be made.

4. Research findings

The introductory statements in each policy were a useful means of revealing a university's broad outlook with regard to information security. Some focussed on the protection of hardware, computer rooms, and other aspects of physical security. Others seemed more concerned about protecting the confidentiality and integrity of their administrative information systems and their administrative data. Still others tended to stress the importance of information for research, and hence their focus was on the protection of such information and of ensuring that their security management regulations helped research endeavours to thrive and to be secured against attack. Because of the high degree of variation with respect to the broad focus, of the reviewed policies, it is not perhaps surprising that there was also a significant degree of variety with regard to the policies' structural arrangements and coverage, as discussed in more detail in the remainder of this section.

4.1. Policy structure

As indicated earlier, the literature on information security policy formulation suggests that organisations typically adopt one of three principal approaches to the structure and format of their policy documentation. The first of these approaches is to create one comprehensive information security policy, containing detailed coverage of each of the risk areas and each security management issue relevant to the organisation in question (Lindup, 1995). The second approach is to create a series of inter-related, cross-referenced, policies: e.g. separate system, product, community and corporate information policies (Baskerville & Siponen, 2002). The third approach is to create an information security policy, supplemented by a number of related guidelines or procedures, typically with each guideline or procedure documents being focussed on one specific aspect of security management (Dhillon, 1997; Rees et al., 2003).

The findings of our review of university information security documentation revealed that a rather different approach was favoured by the majority of universities (see Table 3). Typically, we found that universities tended to have an information security policy, accompanied by a number of related policies, and then also supplemented by a number of specific guidelines and/or practice-related documents. The most typical combination of policies was an information security policy, accompanied by an acceptable use policy and an electronic mail policy. The acceptable use policies tended to cover issues relating to the permissions and prohibitions on the use of university computing facilities by individual members of the university. The electronic mail policies were generally focussed on issues pertaining to permissions and prohibitions regarding the sending of mass emails to large numbers of the university community, and the sending of non-work-related emails, as well as matters relating to email monitoring by university authorities, and email disposal and retention. By and large, the supplementary guidelines and/or procedures tended to address issues with a strong technical orientation. Common examples included permissions and prohibitions on laptop connection to organisational networks, Systems and Network Security Standards, the use of wireless technology, and the disposal of hardware and software.

This finding regarding policy combinations and supplementary documentation generally held true across the various countries in the sample. However, in addition to having acceptable use policies and electronic mail policies, it was noticeable that universities in the USA were more likely also to have in place a privacy policy than were universities from other countries in our sample. For example, only 2 out of the 18 sampled UK universities had a privacy policy, in comparison with 21 out of the 26 US-based universities. These policies tended to cover issues relating to the rights to privacy protection of both data and electronic communications that users can expect as members of the university community, as well as the actions that the university is authorised to take with regard to monitoring and checking data and electronic communications.

4.2. Policy coverage

The analysis of specific security management issues addressed in the universities' security documentation, only considered the institutions' core information security policy, and therefore any supplementary policies/guidelines/procedures were not explicitly reviewed. Each information security policy was thoroughly reviewed to determine its coverage of the key risk areas/security management issues highlighted by Fulford and Doherty (2003). In some cases, a policy might have referred a reader to a

Table 4
The coverage of IS policies.

	Coverage in ISPs	Coverage in ISPs [%]
Security issue		
Violations and breaches	51	84%
User access management	44	72%
Contingency planning	31	51%
Physical security	29	48%
Disclosure of information	22	36%
Viruses, worms, etc.	21	34%
Encryption	14	15%
Mobile computing	11	18%
Software development	10	16%
Personal usage of information	8	13%
Internet access	5	8%
Extra issues		
Responsibilities	41	67%
Enforcement	33	54%
Awareness and training	23	38%
Compliance with legislations	21	34%
Information classification	13	21%
BS (1)7799 reference	12	20%

supplementary policy, in which case this was deemed to be explicit coverage as the reference point was from the core information security policy. Issues covered in separate policies or procedures, but not explicitly mentioned in the information security policy, were not deemed to constitute explicit coverage in our examination, as it has been argued that the information security policy should be the point of departure for addressing all information security issues (von Solms & von Solms, 2004).

Findings for this part of the study showed (see Table 4), first that no one individual policy area was common to all of the universities in the sample. The most extensively covered issues – in descending order – were for the following: violations and breaches; user access management; contingency planning; and physical security. A plausible explanation for the high ranking of violations and breaches, and user access management is that institutions, such as universities, have a range of user types (e.g. research staff, teaching staff, administrative and clerical support staff, as well as a disparate student body). This wide range of user types brings with it the need for a variety of different access points to organisational information systems and networks, such as: staff offices, computer labs, wireless access, research laboratories, campus student accommodation and remote access. Such a wide variety of access points is likely to leave a university's information systems, and the data and information contained in them, vulnerable to security breaches. The range of locations in which computing facilities are available at universities may also serve to explain the reasonably high ranking evidenced in the study for physical security (ranked 4th).

Those areas receiving least coverage in the university information security policies examined in the study were: software development and maintenance (ranked 9th out of the 11 policy areas), personal usage of information systems (ranked 10th), and Internet access (ranked 11th). The low ranking of areas such as the personal usage of information systems and Internet access may be explained by the fact that these are covered in separate procedures and/or guidelines – such as the '*acceptable use*' and '*email*' policies – at a number of the universities in the sample. However, we would argue that even if such issues are adequately covered elsewhere, they should still be explicitly referenced from the information security policy, so that it maintains its position as the central reference point for all security issues. Software development is also covered in only a few of the university information security policies in the sample, and is also not addressed to any great extent in associated policies and/or procedures. This may be because systems development is considered to be a specialised activity that is not typically relevant to the wider organisation. However, this may be a dangerous strategy, as universities tend to allow a certain amount of freedom for members of their community to create their own software. For example, if research teams develop their own simple database applications, to store and analysis their research data, it is still important that such applications are adequately protected. Personal usage may also rank relatively lowly as there is typically a high level of flexibility in universities, particularly in research-related roles, with regard to working hours and working practices, and boundaries between personal usage and work-related activities may sometimes be blurred. It may, therefore, be deemed to be difficult to regulate strictly the personal usage of IS in a university context.

In addition to the policy areas identified by Fulford and Doherty (2003), it was evident from our analysis of the individual university security policies in the sample that a number of other areas were explicitly covered. The most prevalent supplementary issue addressed was employee responsibilities with respect to information security, which is a positive finding, as it supports the view of Gaston (1996, p. 175) that a well written policy should: '*assign the responsibilities that various departments and individuals have in achieving policy goals*'. However, there is little point in clearly delineating responsibilities if it is not made clear to employees how they will be held to account for their discharge, and therefore it is encouraging to find that many universities now explicitly articulate how their policies will be enforced.

Another important area given prominent coverage in many, but by no means all policies is that of information security training and security policy awareness. This held true across all the various countries in the sample with the exception of the USA where there was evidence of less emphasis on training and security awareness, and rather more emphasis on issues pertaining to privacy, monitoring, intellectual freedom and confidentiality. The growing emphasis on training and security awareness is a generally encouraging finding, because unless users are aware of their policy's content, it is likely to become a '*dead*' document (Siponen, 2000). What is perhaps less encouraging is that not only do the information security policies tend cover only a small subset of the areas identified in the framework proposed by Fulford and Doherty (2003), but also that coverage still tends to be restricted, even when all the information security documentation for each institution is examined in its entirety (i.e. the additional policies as well as the supplementary procedures and/or guidelines).

With regard to the underlying objectives of information security management (Dhillon & Torkzadeh, 2006) reflected in their information security policies, there was a high degree of consistency, as can be seen from the evidence presented in Table 5. Most universities' policies had a very strong technical orientation, with their stated objectives focussing on issues such as the need for strict access control, and the paramount importance of maximising the privacy and the integrity of their data assets. By contrast, far less explicit attention was accorded to the socio-organisational aspects of information security, such as the need to develop human resource and management practices, or the need to foster and sustain an ethical environment. A similar trend was found when examining underlying '*principles*' (Dhillon & Backhouse, 2000), that were reflected in the content of our sample of policies. There was a very strong emphasis on information availability, confidentiality and integrity, but very little evidence of any explicit concern for trust, ethicality or organisational integrity. The one recurring principle that did have a more socio-organisational orientation was '*responsibility*', as nearly all the reviewed policies clearly identified the specific responsibilities of different employees, or groups of employees, with respect to the maintenance of information security.

Table 5
The stated objectives of information security policies.

	Objectives of information security policies (based upon Dhillon & Torkzadeh, 2006)	Number of policies
A	Enhance management development practices	14
B	Provide adequate human resource management practices	0
C	Develop and sustain an ethical environment	0
D	Maximise access control	44
E	Promote individual work ethic	9
F	Maximise data integrity	36
G	Enhance integrity of business processes	31
H	Maximising privacy	28
I	Maximise organisational integrity	0

Table 6
Policy content for universities versus policy content for large organisations.

Policy area	Policy content in universities	Policy content in large organisations (Fulford & Doherty, 2003)
Violations and breaches	84%(1)	85%(4)
User access management	72%(2)	91%(1)
Contingency planning	51%(3)	56%(8)
Physical security	48%(4)	83%(5)
Disclosure of information	36%(5)	82%(6)
Viruses, worms, etc.	34%(6)	87%(joint 3)
Encryption	23%(7)	35%(10)
Mobile computing	18%(8)	61%(7)
Software development	16%(9)	53%(9)
Personal usage of information	13%(10)	87%(joint 3)
Internet access	8%(11)	90%(2)

Note: Figures in brackets relate to the relative rank of each policy area.

When it comes to finding any clear evidence that our sample of universities have explicitly tailored their information security policies to take account of their position as knowledge-intensive organizations, there was extremely little to be found. Only four of the reviewed policies [7%] contained any explicit recognition that information security should be accorded a particularly high priority on account of the host organisation's knowledge-intensive status. Where such references did exist, these were typically restricted to brief statements in the policy's introduction, such as: '*information is a vital asset to any organisation, and this is especially so in a knowledge-driven organisation such as the University*'. However, there was absolutely no evidence of any University explicitly tailoring specific policy issues to take account of the knowledge-intensive context in which their policies will be applied.

4.3. Coverage comparison with other types of organisation

A comparison of the policy areas covered in the university policies was made with the areas covered in the large commercial organisations investigated in the Fulford and Doherty (2003) study (see Table 6). It is interesting to note that there are significant differences both in terms of the rankings of the incidence of specific policy issues, as well as the overall levels of coverage. Starting with the overall levels of coverage, it is clear that the policies reviewed in the prior study were generally reported to cover a broader range of issues, than those reviewed as part of our sample of university policies. Indeed, whilst the probability of a specific issue being covered in the original sample was 0.74, it was only 0.36 amongst our sample of university policy. This is a potentially worrying result as it might be anticipated that universities would have more complete and comprehensive policies than other types of enterprise, given the central importance of information and technology to their primary activities of teaching, research and scholarship (Mok, 2005).

In terms of the differences in the prevalence of specific policy issues, between the two samples, perhaps the most noticeable differences were in the coverage of Internet access (ranked 11th in the university study, but 2nd in the study of other organisations) and personal usage of IS (ranked 10th in the university study and joint 3rd in the study of other organisations). These differences can perhaps be explained by the points made earlier in this section regarding the flexibility of IT usage and working Practices in universities, as well as the range of user types in such institutions. As there is generally a high degree of flexibility in the working environment in universities, and as the boundaries between work and personal usage may sometimes become blurred, universities may find it difficult to regulate on these areas and to clearly articulate where the boundaries of IS and Internet usage lie. Alternatively, it may be that universities prefer to focus attention on these issues of personal usage and Internet access by making them the subject of a separate policy (e.g. an acceptable use policy). However, if the latter is the case, it would seem strange to make absolutely no mention of '*personal usage*' or '*Internet access*' within the core information security policy, as the policy is meant to be the '*foundation of*' (Higgins, 1999) and '*at the heart of*' (von Solms & von Solms, 2004) effective security management practices.

It should also be noted that the differences in research methodologies employed may also explain at least some of the identified differences in coverage between university information security documentation and that of other organisations. In this university-focused study, the method employed has been objective, third-party analysis of policy documentation. By contrast, the study in other organisations, was undertaken using questionnaire surveys dependent on an informant within each organisation to provide a reliable and truthful account of their organisation's security management coverage. It may be that these respondents perceived their organisation's coverage to be more extensive than is actually the case. It would, however, prove problematic to test this, as commercial organisations, unlike universities do not tend, for reasons of commercial confidentiality, to make their information security documentation available in the public domain.

5. Discussion

The study reported in this paper makes a number of important contributions to the literature, particularly through its objective critique of the content of information security policies and the

structural configuration of information security documentation. By focussing on the content of employee-oriented security documentation, this study helps to overcome one of the most common criticisms of information security research that it is too technical in its orientation (e.g. Besnard & Arief, 2004; de Paula et al., 2005; Wiant, 2005). Against this backdrop, the aim of this section of the paper is to explicitly articulate this study's contributions, before identifying its implications for the manager and the researcher.

In terms of its contributions to the literature, perhaps the study's most important one, lies in providing one of the first, if not the first, independent and objective review of the coverage of information security policies. The study has demonstrated that the coverage of information security policies, in terms of the numbers of issues explicitly addressed, is typically rather modest, particularly when judged against the prescriptions from the literature and the International Standards (Fulford & Doherty, 2003; ISO, 2005). Neither have the information security policy documents reviewed been found to effectively play their role in co-ordinating the organisations' suite of security documentation, as they do not adequately reference complementary policies and standards. If these findings are indicative of a wider trend, this might help to explain the growing concern that many commentators have expressed over the effectiveness of the information security policies (e.g. Doherty & Fulford, 2005; Hone & Eloff, 2002b; Karyda et al., 2005). Moreover, this study provides some useful insights, from an empirical perspective, into the on-going debate concerning the '*ideal*' structural arrangements with respect to the security documentation (e.g. Lindup, 1995; Siponen, 2000; Sterne, 1991). Whilst the study has highlighted a reasonable variety of practices, which is probably to be expected in an environment where tailoring of policies is argued to be important (Dhillon, 2004), the most common arrangement is for a broad, high-level information security policy, supported by an '*acceptable usage policy*' and a number of more detailed procedures and standards.

Another important contribution of this research has been in our evaluation of the underlying information security management objectives and principles (Dhillon & Backhouse, 2000; Dhillon & Torkzadeh, 2006) reflected in information security policies. It was not perhaps greatly surprising to find that our sample of policies still reflect a highly techno-centric view of information security management, given the technical orientation of the majority of security standards. However, it does highlight the need for both academics and practitioners to explore ways in which the socio-organisational dimensions of information security can be better reflected in policy documents. A final theoretical contribution of this study comes from our focus on Universities, which face a particularly difficult challenge when it comes to the security of their computer-based assets: on the one hand information and knowledge needs to be viewed as a highly competitive resource whose confidentiality must be fiercely protected, whilst on the other, unless these assets are freely shared amongst collaborating colleagues, then their value is unlikely to be leveraged (Desouza & Vanapalli, 2005; Johannessen & Olsen, 2003). Unfortunately, there is no evidence from this study, either in terms of the language used or the coverage of issues, to suggest that universities have tailored their policies to reflect their status as knowledge-intensive organisations.

In terms of its implications for practitioners, then the clear message to be derived from this study is that universities need to critically reappraise their policies to ensure that the coverage is more comprehensive and that it has been explicitly tailored to take account of the critical role of information in the work of the academic. Moreover, in an environment where the variety of distinct documents that address information security is growing rapidly, then the information security policy needs to regain its position of primacy, in which it acts as the point of departure for all the other procedures and policies. The study also has some important implications for the researcher, not only in terms of its novel insights into the scope and coverage of the information security policy, but also with respect to the formulation of policies. Baskerville and Siponen (2002) have previously highlighted the significant gap in the literature with respect to approaches to the formulation of the information security policy. One of the key reasons that this particular literature is underdeveloped may be due to the lack of clarity with regard to the structure and coverage of security documentation. Consequently, a final important contribution of this study may well be in its provision of clear empirical evidence, with respect to the content of information security policies, that can be used to help guide and inform the creation of new approaches to the formulation of future policies.

6. 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 evaluation of the content of authentic information security policies and the structural arrangements of information security documentation, within a well-bounded organisational setting. In so doing, it highlights some worrying deficiencies in terms of the explicit coverage of policy issues and the ability of organisations to effectively cross-reference and integrate their portfolios of information security documentation. Research into the adoption of sophisticated policies, within a dynamic organisational 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, to help interpret and explain the results of our documentation review, are currently being planned. In particular, we are keen to explore how the content of the policies reflects, and aligns with, the universities' strategic planning process. As the project unfolds, it is anticipated that the findings will help organisations to better understand the value of security policies and to pinpoint the policy areas for prioritisation.

References

Arnesen, D. W., & Weis, W. L. (2007). Developing an effective company policy for employee Internet and email use. *Journal of Organizational Culture, Communications and Conflict*, *11*(2), 53–67.

Austin, R. D., & Darby, C. A. (2003). The myth of secure computing. *Harvard Business Review*, *81*(6), 120–126.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organisations. *Information Management and Computer Security*, *15*(5/6), 337–346.

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security*, *23*, 253–264.

Brynjolfsson, E., & Hitt, L. (1996). Paradox lost? Firm-level evidence on the returns to information systems. *Management Science*, *42*(4), 541–558.

Calder, A., & Van Bom, J. (2006). *Implementing information security based on ISO 27001/ISO 17799*. Van Haren Publishing.

Churchill, G. A., Jr. (1997). *Marketing research, methodological foundations*. The Dryden Press.

David, J. (2002). Policy enforcement in the workplace. *Computers and Security*, *21*(6), 506–513.

Desouza, K. C., & Vanapalli, G. K. (2005). Securing knowledge in organizations: Lessons from the defence and intelligence sectors. *International Journal of Information Management*, *25*, 85–98.

Dhillon, G. (1997). *Managing information systems security*. London: Macmillan Press.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125–128.

Dhillon, G. (2004). Realizing benefits of an information security program. *Business Process Management Journal*, *10*(3), 21–22.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(3), 293–314.
Doherty, N. F., King, M., & Al-Mushayt, O. (2003). The impact of inadequacies in the treatment of organizational issues on information systems development projects. *Information and Management*, *41*(1), 49–62.
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.
D.T.I. (2004). *Information security breaches survey*. Department of Trade & Industry.
Drucker, P. F. (1988). The coming of the new organization. *Harvard Business Review*, *66*(1), 45–53.
Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations. *Information Management and Computer Security*, *11*(3), 106–114.
Gaston, S. J. (1996). *Information security: Strategies for successful management*. Toronto: CICA.
Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of information security breaches. *Information Management and Computer Security*, *11*(2), 74–83.
Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377–397.
Higgins, H. N. (1999). Corporate system security: Towards an integrated management approach. *Information Management and Computer Security*, *7*(5), 217–222.
Hinde, S. (2002). Security surveys spring crop. *Computers and Security*, *21*(4), 310–321.
Hone, K., & Eloff, J. H. P. (2002a). Information security policy—What do international security standards say. *Computers & Security*, *21*(5), 402–409.
Hone, K., & Eloff, J. H. P. (2002b). What makes an effective information security policy. *Network Security*, *20*(6), 14–16.
Hong, K., Chi, Y., Chao, L., & Tang, J. (2006). An empirical study of information security policy on information security elevation on Taiwan. *Information Management and Computer Security*, *14*(2), 104–115.
I.S.O. (2005). *Information technology-Security Techniques—Code of practice for information security management-ISO 17799*. Geneva: International Standards Organization.
Johannessen, J.-A., & Olsen, B. (2003). Knowledge management and sustainable competitive advantages: The impact of dynamic contextual training. *International Journal of Information Management*, *23*, 277–289.
Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information security policies: A contextual perspective. *Computers & Security*, *24*(3), 246–260.
Kotulic, A. J., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information and Management*, *41*(5), 597–607.
Lindup, K. R. (1995). A new model for information security policies. *Computers & Security*, *14*, 691–695.
Loggie, K. A., Barron, A. E., Gulitz, E., Hohlfeld, T. N., Kromrey, J. D., & Venable, M. (2006). An analysis of copyright policies for distance learning materials at major research universities. *Journal of Interactive Online Learning*, *5*(3), 224–231.
Markus, M. L. (2004). Techno-change management: Using IT to drive organizational change. *Journal of Information Technology*, *19*(1), 4–20.
Mok, K. H. (2005). Fostering entrepreneurship: Changing role of government and higher education governance in Hong Kong. *Research Policy*, *34*, 537–554.
Moule, B., & Giavara, L. (1995). Policies, procedures and standards: An approach for implementation. *Information Management and Computer Security*, *3*(3), 7–16.
de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D. F., et al. (2005). In the eye of the beholder: A visualization-based approach to information security. *International Journal of Human-Computer Studies*, *63*, 5–24.
Peppard, J. (2007). The conundrum of IT management. *European Journal of Information Systems*, *16*, 336–345.
Porter, M. E., & Millar, V. (1985). How information gives you competitive advantage. *Harvard Business Review*, *63*(4), 149–160.
Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: A policy framework for information security. *Communications of the ACM*, *46*(7), 101–106.
Saleh, M. S., Alrabiah, A., & Saad, H. B. (2007). Using ISO 17799; 2005 Information Security Management: A STOPE view with six sigma approach. *International Journal of Network Management*, *17*(1), 85–97.
Sheehan, N. T., & Stabell, C. B. (2007). Discovering new business models for knowledge-intensive organizations. *Strategy & Leadership*, *25*(2), 22–29.
Siponen, M. (2000). Policies for construction of information systems' security guidelines. In *Proceedings of the 15th international information security conference (IFIP TC11/SEC2000)* Beijing, China, August, (pp. 111–120).
Siponen, M. T. (2005). An analysis of traditional IS security approaches: implications for research and practice. *European Journal of Information Systems*, *14*(3), 303–315.
Sircar, S., & Choi, J. (2007). A study of the impact of information technology on firm performance: A flexible production function approach. *Information Systems Journal*, doi:10.1111/j.1365-2575.2007.00274.x
von Solms, B., & von Solms, R. (2004). The ten deadly sins of information security management. *Computers & Security*, *23*, 371–376.
Sterne, D. F. (1991). On the buzzword 'security policy'. In *Proceedings of the IEEE symposium on research in security and privacy* (pp. 219–230).
Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441–470.
THES. (2007). World University Rankings, November 5, 2007. *The times higher education supplement*. Available at: http://www.timeshighereducation.co.uk/Magazines/THES/graphics/WorldRankings2007.pdf Accessed December, 2007.
du Toit, A. S. A. (2003). Competitive intelligence in the knowledge economy: What is in it for South African manufacturing enterprises. *International Journal of Information Management*, *23*, 111–120.
Wadlow, T. A. (2000). *The process of network security*. Reading, MA: Addison-Wesley.
Ward, J., & Peppard, J. (2002). *Strategic planning for information systems*. Chester: Wiley.
Wiant, T. L. (2005). Information security policy's impact on reporting security incidents. *Computers & Security*, *24*(6), 448–459.
Whitman. (2004). In defense of the realm: Understanding threats to information security. *International Journal of Information Management*, *24*, 3–4.
Zammuto, R. F., Griffith, T. L., Majchrzak, A., Dougherty, D. J., & Faraj, S. (2007). Information technology and the changing fabric of organization. *Organization Science*, *18*(5), 749–762.

Professor Neil Doherty currently holds the Chair in Information Management in the Business School at Loughborough University. In addition to information security, his research interests include the interaction between organisational issues and technical factors in information systems development, understanding the reasons for failures of information systems projects, strategic information systems planning, benefits realisation management and electronic commerce. Neil has had papers published in a range of academic journals, including: *European Journal of Information Systems*, *Journal of Information Technology*, *Journal of Strategic Information Systems*, *Information Resources Management Journal*, *IEEE Transactions in Engineering Management*, *Journal of Business Research*, *European Journal of Marketing*, *Journal of End User Computing*, *Information Technology & People, Behaviour & IT and Information & Management*. Professor Doherty is currently serving as an associate editor for *Information Technology and People* and the *International Journal of Electronic Business Research*.

Dr Leonidas Anastasakis is a research associate in the Management Science and Information Systems research group at Loughborough University Business School. Prior to joining Loughborough University, he gained a PhD (Financial Prediction) and an MSc (Control Systems) degrees at the University of Sheffield, following on from undergraduate studies at the Technological Educational Institute of Piraeus, Greece. His research interests are in the areas of forecasting, information security management and the adoption of e-commerce. His work has appeared in the *Journal of the Operational Research Society, Expert Systems with Applications* and in a number of international conferences.

Dr Heather Fulford is a reader in Entrepreneurship in the Charles P. Skene Centre for Entrepreneurship (CfE) at Aberdeen Business School, and a Visiting Fellow, at the Business School, Loughborough University. Dr Fulford's research interests include: IT in small businesses; electronic commerce adoption and diffusion in SMEs; innovation diffusion; language and translation technologies; website design and development and information security management. Dr Fulford is currently a board member of the following journals: European Journal of Innovation Management; Journal of Specialised Translation and the Encyclopedia of Information Ethics and Security. Heather has had her papers published in a range of academic journals, including: *Information Management & Computer Security*, *Information Resources Management Journal, Computers & Security, International Journal of Retail & Distribution Management and Terminology*. *Journal of Consumer Marketing, International Journal of Entrepreneurship Innovation*, and *Journal of Enterprising Culture*.