available at www.sciencedirect.com

SCIENCE DIRECT®

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

Computers & Security

Aligning the information security policy with the strategic information systems plan

Neil F. Doherty, Heather Fulford*

The Business School, Loughborough University, Ashby Road, Loughborough, Leicestershire LE11 3TU, United Kingdom

ARTICLE INFO

Article history:
Received 2 September 2004
Revised 24 February 2005
Accepted 29 September 2005

Keywords:
Strategic information systems planning
Information security policy
Security breaches
Alignment
Information security management
Information security policy components

ABSTRACT

Two of the most important documents for ensuring the effective deployment of information systems and technologies within the modern business enterprise are the strategic information systems plan (SISP) and the information security policy. The strategic information systems plan ensures that new systems and technologies are deployed in a way that will support an organisation's strategic goals whilst the information security policy provides a framework to ensure that systems are developed and operated in a secure manner. To date, the literature with regard to the formulation of the information security policy has tended to ignore its important relationship with the strategic information systems plan, and vice versa. In this paper we argue that these two important policy documents should be explicitly and carefully aligned to ensure that the outcomes of strategically important information system initiatives are not compromised by problems with their security.

© 2005 Elsevier Ltd. All rights reserved.

1. Introduction

For the past two decades it has been argued that an '*information revolution*' is taking place that is having a significant impact upon all aspects of organisational life (e.g. Porter and Millar, 1985; Drucker, 1988). Indeed, it is often contended that information is now analogous to an organisation's lifeblood: should the flow of information become seriously restricted or compromised then the organisation may wither and die. However, if applied effectively as a strategic resource, information investments can result in the realisation of significant corporate benefits. As McPherson (1996) argues, '*information is vital to the success of the business and will be accountable for a significant share of the business's various indicators of success, including its cash flow and market value*'. However, such benefits will not be realised from the utilisation of information if the associated information systems and technologies are applied in an unfocussed and piecemeal way. As Lederer and Sethi (1996) note, strategic information systems planning (SISP) plays a vital role in helping to avoid '*lost opportunities, duplicated effort, incompatible systems, and wasted resources*'. Looked at in a different way, the process of formulating an information systems plan helps to explicitly focus the planners' attention on '*major opportunities for exploiting information*' (Ward and Peppard, 2002; p. 468).

Whilst a key objective of strategic information systems planning is to identify opportunities to exploit information, Ward and Peppard (2002; p. 468) also note that the real '*challenge is to ensure that this information is of the highest quality possible, particularly in terms of timeliness, accuracy, completeness, confidence in source, reliability and appropriateness*'. Unfortunately, in practice, many organisations are failing to

* *Corresponding author*. Tel.: +44 1509 223128; fax: +44 1509 223960.
E-mail address: n.f.doherty@lboro.ac.uk (N. F. Doherty)
0167-4048/$ – see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.09.009

consistently provide the high quality information resources that their managers require, because of unacceptably high levels of security breaches experienced (Garg et al., 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 (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%–10% of its IT budget on security*'. One important mechanism for protecting corporate information, in an attempt to detect, prevent and respond to security breaches is through the formulation and application of an information security policy (InSPy) (Hone and Eloff, 2002; von Solms and von Solms, 2004).

There is therefore an obvious relationship between strategic information systems planning and information security management, and hence between the two key documents associated with these activities: the strategic information systems plan and the information security policy. The former document is designed to identify what information resources are required and how they can be exploited, whilst the latter details how such information can be kept secure and therefore readily available to managers. For example, if a strategic information systems plan were to identify the need for an enterprise-wide intranet, then the information security policy would need to be modified to take account of this highly significant change to the way in which corporate information is to be stored, disseminated and managed.

Higgins (1999) argues that the information security '*policy is the start of security management*'. Whilst supporting this sentiment, we would add the caveat that the strategic information systems plan is a critical prerequisite for policy formulation, as it defines the business context in which information security will be managed and therefore the objectives of, and priorities for, security management. Unfortunately, whilst the relationship between these two key business documents appears clear, a thorough review of the literature suggests that this subject has been given little explicit coverage in academic or practitioner publications. Consequently, the broad aim of this paper is to fill this gap in the literature by exploring how and why the information security policy should be explicitly aligned with the strategic information systems plan. To explore the issue, the remainder of the paper has been organised into a further four sections. The first section ''The relationship between the information security policy and the strategic information systems plan'' reviews the relevant literature, before some common business cases are used to investigate in more detail the nature of the relationship, between SISP and the InSPy, in the section entitled ''Case examples''. In the final sections, we review the implications of our findings in the context of the literature.

2. The relationship between the information security policy and the strategic information systems plan

The purpose of this section is to review the aims and scope of the strategic information systems plan and then the information security policy, before exploring how the two might be directly related.

2.1. *The role and scope of the strategic information systems plan*

As concerns continue to grow about the value and effectiveness of IT investments, improving strategic information systems planning practices has rapidly become one of the most critical issues facing IS executives today (Galliers, 1993; Segars et al., 1998; Newkirk et al., 2003). Strategic information systems planning (SISP) has been defined as: '*the process of identifying a portfolio of computer-based applications to be implemented, which is both highly aligned with corporate strategy and has the ability to create an advantage over competitors*' (Doherty et al., 1999). It is, therefore, an exercise, or ongoing activity, that enables organisations to develop priorities for IS development. Specific projects are chosen for their alignment with business objectives or their capacity to create significant impact on the organisation's competitive positioning. Whilst the main focus of SISP – as witnessed by the above definition – is typically viewed as the identification of new applications, Beynon-Davies (2002; p. 417) suggests that a SISP exercise may cover a wider variety of projects. More specifically, he suggests that SISP facilitates the identification of a prioritised portfolio of the following types of system and technology related projects:

- corrections to existing information systems;
- enhancements to existing information systems;
- major new information systems development projects;
- major new infrastructure systems or technologies, for example those that attempt to integrate systems across the organisation;
- research projects investigating innovative and potentially rewarding systems and technologies.

The implementation of any of the above types of project in a portfolio can have significant implications for the security of corporate information resources, and consequentially the organisation's information security policy. We would, therefore, argue that the output of the strategic information planning process – a comprehensive, fully costed and timetabled plan – should be used to test the adequacy of the current InSPy, if one already exists, or to provide focus for the creation of an initial policy, if it does not exist. A fuller discussion of the process of information systems planning, and how the review of the information security policy might usefully be incorporated, is presented in the section ''The relationship between the information security policy and the strategic information systems plan''.

2.2. *The role and scope of the information security policy*

Gaston (1996; p. 175) suggests that the information security policy can be defined as the '*broad guiding statements of goals to be achieved*' with regard to the security of corporate information resources. This definition is broadly in line with the International Standard on '*Information Security Management*' (ISO 17799, 2000; p. 1), which suggests that the InSPy document

should '*provide management direction and support for information security*'. As such, InSPys typically include '*general statements of goals, objectives, beliefs ethics and responsibilities, often accompanied by the general means of achieving these things (such as procedures)*' (Wood, 1995). The information security policy has become the focus of an increasing amount of academic scrutiny, over the past 10 years or so, as its critical role in preventing, detecting and responding to security breaches has become more apparent. The aim of this section is to provide a review of this body of literature, paying particular attention to the importance and scope of such policies.

There is a growing consensus both within the academic and practitioner communities that the information security policy is the basis for the dissemination and enforcement of sound security practices, within the organisational context (e.g. Baskerville and Siponen, 2002; Doherty and Fulford, 2005). As David (2002) notes: '*it is well known, at least among true security professionals, that formal policy is a prerequisite of security*'. Similarly, Lindup (1995) asserts:

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

The primary reason that the InSPy has become the '*prerequisite*' or '*foundation*' of effective security practices has been suggested by Higgins (1999), who notes: '*without a policy, security practices will be developed without clear demarcation of objectives and responsibilities*'.

Whilst a great deal has been written about the importance and role of the information security policy, and approaches to its formulation and dissemination, there is relatively little academic material that explicitly addresses the scope or content of security policies. One recent attempt to explicitly fill this gap synthesised the key themes from the literature – in particular the international standard (ISO 17799, 2000) – into a list of specific issues to be addressed by the information security policy. This provisional list was then validated through an empirical study of the use of the InSPy, within large UK-based organisations (Fulford and Doherty, 2003). Given that these issues will form the framework for analysing our case examples, in the section "Case examples", we have provided the following working descriptions for each of these individual components of the information security policy:

1. *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.
2. *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.
3. *Physical security of infrastructure and information resources*: It has been noted that '*equipment should be physically protected from security threats and environmental hazards*' (ISO 17799, 2000; p. 16). It is, therefore, important that the policy explicitly articulates how infrastructure and information resources are to be protected.
4. *Violations and breaches of security*: As noted in the introduction to this paper security breaches are still a common, and potentially very damaging, occurrence. The policy document must therefore indicate the steps to be taken to recover from a breach or violation and the requirements for recording such security incidents (ISO 17799, 2000; p. 16).
5. *Prevention of viruses and worms*: The rapid proliferation of viruses, worms and trojans present an increasingly potent threat to the security of corporate information resources (Post and Kagan, 2000; Hinde, 2002). The organisation's policy with regard to the application of virus checking software, the use of attachments and the sharing of information must therefore be made clear.
6. *User access management*: It has been noted that '*access to information and business processes should be controlled on the basis of business and security requirements*' (ISO 17799, 2000; p. 33). The information security policy should, therefore, provide a '*clear statement of the business requirements to be met by access controls*' (ISO 17799, 2000; p. 33).
7. *Mobile computing*: The use of notebooks, palmtops and laptops away from the traditional working environment makes them particularly vulnerable, as they are more difficult to protect using conventional security controls. The policy must therefore highlight the practices that must be adopted to ensure that '*business information is not compromised*' (ISO 17799, 2000; p. 46).
8. *Internet access*: As the use of the Internet – in the workplace – 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.
9. *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 and procedures are built into all new systems.
10. *Encryption*: The growth of electronic commerce and mobile computing has inevitably increased the amount of information that is being communicated across public – and potentially less secure – networks. The organisation's requirements for the encrypting of such information must therefore be clearly addressed in the information security policy.
11. *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 or a serious virus. The information security policy must specify how such contingency plans are to be written, tested, maintained, and ultimately implemented.

The above review has attempted to identify and describe the issues that will commonly be addressed in the information security policy. However, it cannot claim to be either a definitive or generic list, as the range of issues to be covered in a specific policy will very much depend upon the host organisation's particular circumstances and security priorities. It is

likely that any significant modification to an organisation's IT infrastructure and applications – engendered by a new information systems plan – will have an impact on the majority, if not all of the above issues.

2.3. *The relationship between the information security policy and the strategic information systems plan*

A review of the literature suggests that researchers and practitioners are beginning to recognise that the information security policy should relate in some way to corporate objectives. For example, the International Standard (ISO 17799, 2000; p. xi) suggests that the '*security policy should reflect business objectives*'. However, the standard goes on to suggest that a review of the information security policy should take place '*in response to any changes affecting the basis of the original risk assessment, e.g. significant security incidents, new vulnerabilities or changes to the organizational or technical infrastructures*' (ISO 17799, 2000; p. 2). Consequently, the Standard appears to emphasise a reactive form of policy review, and it certainly offers no explicit advice on how the policy might best be aligned with corporate objectives. Zuccato (2004; p. 67) also suggests that the point of departure for the preparation of a security requirements model is the specification of a vision and goals, but he does not specify whether this is the organisational vision and goals, or the vision and goals of the modelling exercise. Whilst Baskerville and Siponen (2002) recognise that information security policies should be '*approved by a steering committee of managers, which may include specialists in information security, design and development and* ***strategic planning***[1], they make no explicit link between the information security policy and corporate objectives.

In summary, whilst there have been isolated calls in the literature for a link between corporate objectives/strategic planning and the formulation of the information security policy, there has been no focussed discussion of how this link might be established and operationalised. One obvious approach – that to the best of our knowledge has not been addressed in either the academic or practitioner literatures – would be to closely and explicitly align the information security policy with the strategic information systems plan, which in turn should be based upon corporate objectives.

Fig. 1 presents a highly summarised view of how the process of reviewing the information security policy might be accommodated within the strategic information systems planning process. In Fig. 1a, we see the traditional process by which the strategic information systems plan is formulated: an appropriate planning team is assembled, the situation analysis is conducted and a strategy is formulated and then implemented. Having implemented the new strategic plan, it will be periodically reviewed and modified to ensure that it is pertinent to the organisation's changing needs. In Fig. 1b this traditional process for formulating the IS plan has been modified to accommodate the information security policy.[2] In this case, once the new strategy has been formulated, its impact on the information security policy will be reviewed – and if necessary the security policy will be modified – prior to the implementation of the strategy. Similarly, when reviewing a new strategy, once it is operational, the impact of any changes on the information security policy will be reviewed, before implementing any changes to the strategy.

As the 'review/*modify information security policy*' phase, on the revised version of the SISP, is probably the most important, in the context of this paper, it warrants some further explanation. It is envisaged that this activity should be operationalised by firstly assembling a group of appropriate personnel – IT, information security, strategic planning and commercial specialists – to review the security implications of the strategy. More specifically, this group should assess the ways in which each individual IT project – documented in the SISP – might be used and abused, once operational, and consequently how each might threaten the security of the organisations' information resources. Having generated a list of potential security threats, in terms of both their likelihood and significance, the existing information security policy must then be critically reviewed to assess whether each of these potential threats is adequately countered by the existing policy. If it is not, then each of the inadequate components must be modified to effectively counter the newly identified threat. Whilst the key focus of this exercise will be the alignment of the strategic information systems plan, and the InSPy, it is recommended that the corporate objectives are also considered, in case there are any changes to the wider corporate strategy that might impact upon information security, even if these haven't been reflected in the SISP. For example, a strategic drive to increase the number of customers using an organisation's website might not warrant any explicit changes to the organisation's IS/IT provision, but it might have indirect implications for information security.

In situations where a policy is not currently in use, this explicit link between SISP and information security, will not only help to get information security on senior managers' agendas, it will also act as a very strong cue for organisations to formulate an initial policy. Indeed, this eventuality is highly likely, as recent findings with respect to the uptake of information security policies within the UK suggest that nearly two-thirds of all companies are still failing to implement a policy (DTI, 2004). Even amongst larger organisations [250+ employees], the level of uptake is still a potential cause of concern (DTI, 2004; Fulford and Doherty, 2003). The most likely explanation for this low level of adoption is that information security is simply not '*high on the agenda of those at board level*' (May, 2003; p. 13).

It could be argued that the review of the information security policy does not need to be so explicitly integrated into the SISP formulation process, as there is likely to be a significant time lag between the formulation of a new strategic IS plan, and any resulting implications for the management of information security. However, we believe that this proactive approach can be defended on the grounds that there may be instances where the introduction of a new strategy will have such a significant impact on the management of information security that it will require changes to the strategy before it is implemented. For example, a new strategy in support of the

[1] Our emphasis.

[2] There is an underlying assumption in our basic model that the organisation already has an information security policy. However, for those organisations that do not, the process of formulating a new IS plan should act as a stimulus for developing an initial information security policy.

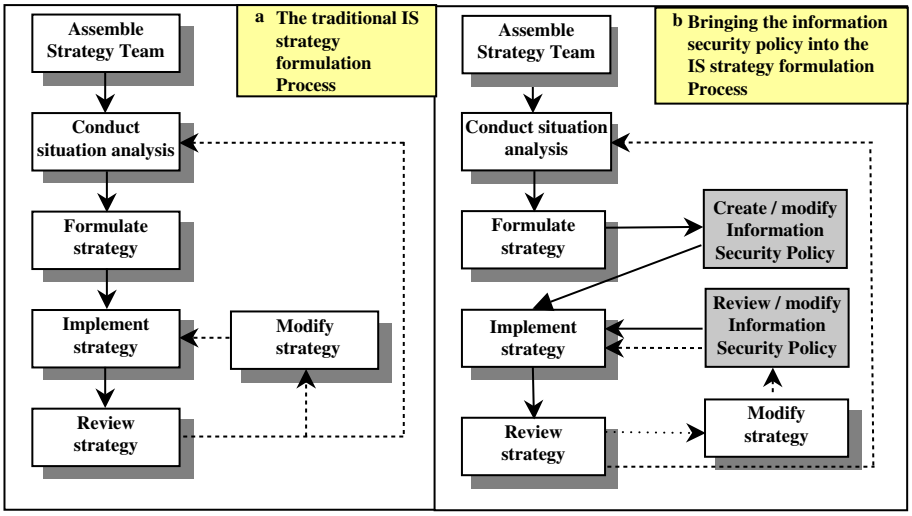

Fig. 1 – From traditional SISP to security-oriented SISP.

introduction of an enterprise-wide intranet might have such significant implications for information security, that it warrants the introduction of a completely new IT infrastructure, which will, in turn, require a significant change to the new strategy to accommodate this. In extreme cases, it could even be that the implications of a new strategic initiative are so potentially dangerous, that the strategy has to be shelved. For example, concerns about ensuring the security of online transactions might dissuade a retailer from developing a web-based ordering facility. Whilst we have argued strongly that the InSPy should be reviewed and updated, in a proactive manner, as an integral part of the strategic information systems planning process, we also recognise that there will still be circumstances where the InSPy will need to be modified in response to a given set of circumstances. For example, if an organisation's information security procedures have been seriously compromised by hackers or viruses, then it may be necessary to immediately modify the policy to reduce the likelihood of repeat occurrences.

3. Case examples

The aim of this section is to explore how the strategic information systems plans for some common types of information systems and technology implementation projects might affect the information security policy of a large manufacturing organisation.[3] For each of these hypothetical projects, the broad strategic objectives of the initiative will be explored, before the implication of each for the formulation of the InSPy is investigated, and in some cases vice versa. The projects outlined range from relatively simple introductions of new hardware or software to a small section of an organisation, through to more complex systems initiatives that are likely to have a considerable impact on working practices across the organisation as a whole, as well as on the organisation's trading partners (suppliers and customers).

3.1. *Example 1: introduction of Internet access to the R&D department*

Organisations are increasingly using the Internet for information retrieval purposes, rather than relying on more conventional paper-based information repositories (DTI, 2004). The introduction of Internet access to the R&D department of a manufacturing organisation would, for example, permit rapid and extensive competitor analysis, and product comparisons. However, as it is typically difficult to restrict Internet usage to very narrowly defined domains, its use, and indeed abuse, can have significant security implications. For example, users may download insecure data and files, view illegal material (e.g. pornography), or simply waste time in non-productive activities. Consequently, those areas of the policy relating to personal IT usage and Internet access will require particularly close scrutiny, as the potential security impacts are likely to be most significant in these areas.

3.2. *Example 2: introduction of laptops to the sales team*

The use of mobile computing facilities, such as laptops, has been a boon for many organisations, allowing their staff to keep in touch with the office whilst off-site, and also giving them remote access to corporate facilities, such as product databases, whilst visiting clients, attending trade fairs, and so on. However, the introduction of laptops and other mobile computing devices has a number of major security implications (Ahlberg, 2004). For example, there is the problem of physical security: the equipment is more vulnerable to theft and damage while staff are away from their office base. There is also the issue of remote access to corporate data resources, which can be vulnerable to attacks from outside as the networks are not likely to be as secure as those used within the

[3] A manufacturing context was explicitly chosen, as manufacturers typically invest in a wide range of often highly sophisticated systems that can have very significant security implications.

organisation itself. Indeed, a recent survey (Ahlberg, 2004) showed that a third of users do not even use simple password protection facilities on their mobile computing devices, whilst two-thirds of mobile computing users did not have their data encrypted. Moreover, as with the previous example, there are likely to be concerns with regard to users' personal use of organisational systems and remote access to the Internet. However, in the case of mobile computing, these concerns may be exacerbated, as staff are away from the normal in-house controls and monitoring regimes. Problems of disclosing information may also be more likely, in situations where users are working off-site, often in close proximity to trading partners. Again, all those areas of the information security policy dealing with these specific security threats will need to be thoroughly reviewed, and where necessary modified, particularly personal usage, mobile computing and Internet access, where the impacts of mobile computing are likely to be most significant.

3.3. *Example 3: ERP implementation*

An enterprise resource planning (ERP) system is a software package with integrated modules that support all major business functions across an organisation. ERP systems have become increasingly popular amongst many commercial organisations, particularly those operating in the manufacturing sector, where they can deliver many benefits (Spathis and Constantinides, 2003). It is very likely that the adoption of an ERP system, within a manufacturing organisation, would have significant implications for the management of corporate information, and in particular the safeguarding of its security. In addition to those security areas already discussed under the first two examples, the organisation is likely to review areas associated with information disclosure, as the ERP will make information more widely available to different types of users across the organisation. Moreover, the organisation may need to establish more comprehensive contingency plans, as an ERP is likely to make the organisation more dependent on its IT resources. Encryption rules will need to be thoroughly reviewed if the organisation is intending to use the ERP to link via electronic networks to suppliers and customers. The latest DTI security breaches survey report notes, for example, that '*greater connectivity*' has increased the '*exposure of UK businesses to security threats*' (DTI, 2004).

In the case of a strategic initiative such as ERP implementation, it is arguably not just the impact of the strategic initiative on the security policy that needs to be reviewed. There may also be cases where it will be necessary to amend the strategic information systems plan, to avoid high risk security problems. For example, most ERP systems are acquired in packaged form, with a wide variety of security controls built in. The organisation will need to consider whether such predefined controls are stringent enough for their purposes, and whether they match the sorts of controls documented in their existing policy. It may be that the organisation decides, at the planning and systems development stage, that certain components of the ERP package are not sufficiently secure for their purposes, and they may decide, therefore, not to implement those components, and perhaps instead to develop their own bespoke components or systems.

3.4. *Example 4: E-commerce initiative*

Through its high levels of connectivity, reach and adoption, the Internet, has probably become the most influential of the vast array of technologies available to businesses. For manufacturing organisations it has provided an unprecedented opportunity for selling products directly to clients (Doherty et al., 2003; De Kare-Silver, 2000).

Electronic commerce is particularly vulnerable to network related threats, such as '*unauthorised access by outsiders*' and '*virus infection and disruptive software*' (DTI, 2004). Consequently, it is very likely that the introduction of a significant e-commerce operation, within a manufacturing organisation, will have significant implications for the management of corporate information, and in particular the safeguarding of its security. One of the key concerns here is that the organisation will be linking itself electronically to its customers, involving increased external e-mail and other Internet-based traffic, leading to the possibility of higher levels of virus and worm attacks, hacking incidents, and various denial of service attacks than were noted in the previous cases. In turn, this means that the organisation needs to ensure that it has adequate contingency and recovery plans in place, including alternative arrangements for customers to place orders when the web-based service is out of action, and so on. Indeed, the DTI survey (2004) found that interruptions to the availability of services were a major problem for many UK businesses, with some organisations suffering a '*very major disruption to their business operations for more than a month*'. A plan for the introduction of a comprehensive, web-based facility might highlight security concerns of such a magnitude, that it is necessary to amend the plan. For example, the introduction of online order tracking, which would entail giving customers access to organisational systems, might be judged to be too risky, as it would expose the organisation to unacceptable security risks from hackers.

The evidence presented in this section is that there is a very strong rationale for reviewing the information security policy in tandem with the formulation of a plan for a significant new, strategic initiative, regardless of the size and scope of that initiative. Table 1 provides a summary of each of the illustrative IT projects, reviewed previously, highlighting the components of the information security policy, which are likely to be most significantly affected by its introduction: the more significant the potential impact, with regard to a specific policy component, then the more thoroughly that component will need to be reviewed. The table highlights the fact that as the IT initiatives increase in complexity, particularly in terms of their impacts both within the organisation, and beyond the organisation to trading partners, the greater the impact on the information security policy and the greater the number of policy components requiring evaluation and possible amendment. It also demonstrates that the security concerns vary greatly between the initiatives and therefore the security implications of each and every new strategy must be judged on its own specific characteristics.

Table 1 – The impact of strategic initiatives on information security policy

Policy components	Case examples			
	Internet access for R&D Department	Laptops for sales team	Introduction of ERP	E-commerce project
Personal usage of information systems	XX	XXX	X	X
Disclosure of information		X	XX	XXX
Physical security of infrastructure and information		XX	XX	XX
Violations and breaches of security	X	X	XX	XXX
Prevention of viruses and worms	XX	XX	X	XXX
User access management	X	XX	XX	X
Mobile computing		XXX		
Internet access	XXX	XXX		
Software development and maintenance			XX	XX
Encryption		X	XX	XXX
Contingency/continuity planning			XXX	XXX

Key: X: limited impact; XX: moderate impact; XXX: highly significant impact.

4. Discussion

Unfortunately, it has often been observed that the high levels of security breaches experienced by commercial organisations – as discussed in this paper's introduction – are failing to raise the organisational profile of information security management. As Straub and Welke (1998; p. 441) note:

> 'Information security continues to be ignored by top managers, middle managers, and employees alike. The result of this unfortunate neglect is that organizational systems are far less secure than they might otherwise be and that security breaches are far more frequent and damaging than is necessary'.

We would argue that the explicit alignment of the information security policy with the strategic information systems plan might be one constructive way of making information security more relevant and meaningful to managers, which in turn might help to reduce the incidence and severity of security breaches. In adopting this approach organisations can move from a reactive style of security management to a far more proactive one. More specifically, it is envisaged that the alignment of these two important strategic documents might deliver the following six benefits:

1. The recent DTI (2004) report concluded that '*all too often, an organisation's security policy is out of step with the current business priorities*'. The explicit alignment of the SISP formulation, and the InSPy creation review, processes will help to give the security policy a far stronger business orientation.
2. The information security policy can be modified in advance of a new strategic information systems initiative to ensure that its implementation does not create any new and unexpected security risks.
3. A 'proactive security culture' is unfortunately very rare (May, 2003; p. 11), with the consequence that the InSPy is typically updated in response to security breaches, or technological changes. The integrated approach will allow the InSPy to be modified in a more proactive manner, and in so doing shift the emphasis from rectification, to prevention.
4. Prior to its implementation, the strategic information systems plan can be reviewed and modified – from a security perspective – to avoid the introduction of any information systems/technology initiatives that would be open to significant information security risks.
5. By reviewing the strategic information systems plan and the information security policy in parallel it will be possible to flag-up important security controls that need to be built into new systems that have been identified in the information system plan, in advance of their development. In a similar vein, it will also be possible to incorporate security management issues into user manuals, training documentation and procedures prior to the introduction of new systems.
6. It has long been recognised that the real threat from security breaches lies in their consequential impact on organisational performance, such as damage to customer confidence or a loss in sales revenues (e.g. Menzies, 1993). By integrating the InSPy review into information systems planning, which is a business oriented exercise, it should be possible to raise managers' awareness of the consequential impacts of security breaches and to consider how they can best be countered through the InSPy.

In terms of the limitations of the proposed approach, the key deficiency, at present, is that our proposals are purely

theoretical. Consequently, we need to test our proposal in practice and gain insights from any organisations that have already investigated integrating their InSPys into their information systems planning process. We also need to develop a deeper understanding of exactly how the link between the strategic information systems plan and the information security policy might best be operationalised. Moreover, it will be important to also explore whether there may be any alternative approaches to the alignment of the InSPy with corporate objectives. Follow-up research projects, adopting an action research approach, are currently being planned to help fill these gaps in our knowledge.

5. Concluding remarks

A recent piece of research (Watson, 2004) suggests that the security of IT systems is the most stressing problem facing IT Directors. It is envisaged that the explicit integration of the InSPy review into the strategic information systems planning process, might provide IT Directors with a powerful and effective new approach to improving the security of their systems. In so doing, it should help to ensure that the information security policy is not '*an IT document designed by IT in isolation from the business*' (Hinde, 2002; p. 315). When reviewing our proposals, however, it must, be remembered that that this is an exploratory piece of research designed, at this stage, to prompt a debate rather than to provide any complete answers.

REFERENCES

Ahlberg M. Data goes walkabout. The Computer Bulletin 2004; 46(6):24–5.

Austin RD, Darby CA. The myth of secure computing. Harvard Business Review 2003;June:121–6.

Baskerville R, Siponen M. An information security meta-policy for emergent organisations. Information Management and Computer Security 2002;15(5/6):337–46.

Beynon-Davies P. Information systems. Basingstoke: Palgrave; 2002.

David J. Policy enforcement in the workplace. Computers & Security 2002;21(6):506–13.

De Kare-Silver M. E-shock 2000, The electronic shopping revolution: strategies for retailers and manufacturers. Basingstoke: Macmillan Business; 2000.

Doherty NF, Fulford H. Do information security policies reduce the incidence of security breaches: an exploratory analysis. Information Resources Management Journal 2005; 18(4):21–38.

Doherty NF, Marples CG, Suhaimi A. The relative success of alternative approaches to strategic information systems planning: an empirical analysis. Journal of Strategic Information Systems 1999;8(3):263–83.

Doherty N, Ellis-Chadwick FE, Hart CA. An analysis of the factors affecting the adoption of the Internet in the UK retail sector. Journal of Business Research 2003;56(11):887–97.

Drucker PF. The coming of the new organisation. Harvard Business Review 1988; Jan–Feb.

DTI. Information security breaches survey. Department of Trade & Industry; 2004.

Fulford H, Doherty NF. The application of information security policies in large UK-based organisations: an exploratory analysis. Information Management and Computer Security 2003;11(3):106–14.

Galliers RD. Research issues in information systems. Journal of Information Technology 1993;8:92–8.

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

Gaston SJ. Information security: strategies for successful management. Toronto: CICA; 1996.

Higgins HN. Corporate system security: towards an integrated management approach. Information Management and Computer Security 1999;7(5):217–22.

Hinde S. Security surveys spring crop. Computers & Security 2002; 21(4):310–21.

Hone K, Eloff JHP. Information security policy – what do international security standards say? Computers & Security 2002; 21(5):402–9.

ISO. Information technology. Code of practice for information security management – ISO 17799. International Standards Organization; 2000.

Lederer AL, Sethi V. Key prescriptions for strategic information systems planning. Journal of Management Information Systems 1996;13(1):35–62.

Lindup KR. A new model for information security policies. Computers & Security 1995;14(8):691–5.

May C. Dynamic corporate culture lies at the heart of effective security strategy. Computer Fraud & Security 2003;2003(5): 10–3.

McPherson PK. The inclusive value of information. International Federation for Information and Documentation – 48th congress. Graz; 1996. p. 41–60.

Menzies R. Information systems security. In: Peppard J, editor. IT strategy for business. London: Pitman Publishing; 1993.

Newkirk HE, Lederer AL, Srinivasan C. Strategic information systems planning: too little or too much? Journal of Strategic Information Systems 2003;12:201–28.

Porter ME, Millar VE. How information gives you competitive advantage. Harvard Business Review 1985;Jul–Aug:149–60.

Post G, Kagan A. Management trade-offs in anti-virus strategies. Information & Management 2000;37(1):13–24.

Segars A, Grover V, Teng T. Strategic information systems planning: planning system dimensions, internal co-alignment, and implications for planning effectiveness. Decision Sciences 1998;29(2):303–41.

Spathis C, Constantinides S. The usefulness of ERP systems for effective management. Industrial Management and Data Systems 2003;103(9):677–85.

von Solms B, von Solms R. The ten deadly sins of information security management. Computers & Security 2004;23(5): 371–6.

Straub DW, Welke RJ. Coping with systems risk: security planning models for management decision making. MIS Quarterly 1998; 22(4):441–70.

Ward J, Peppard J. Strategic planning for information systems. Chichester: John Wiley & Sons; 2002.

Watson J. CIO's feel the strain of business alignment. Computing 26 August 2004:5.

Wood CC. A policy for sending secret information over communications networks. Information Management and Computer Security 1995;4(3):18–9.

Zuccato, A. Holistic security requirements engineering for electronic commerce. Computers & Security 2004;12(1):63–76.

Dr. Neil F. Doherty is a senior lecturer in Information Systems 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 and e-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, Journal of End User Computing, Information Technology & People, Behaviour & IT and Information & Management*.

Dr. Heather Fulford is a lecturer in Information Systems in the Business School at Loughborough University. Her research interests include security management in large and small enterprises, electronic commerce adoption, web site design, and knowledge management. She is currently managing an EPSRC-funded project investigating the adoption of IT by UK SMEs, and has also gained government funding for an e-commerce adoption project. Heather has had her papers published in a range of academic journals, including: *Information Management & Computer Security, Information Resources Management Journal, International Journal of Retail & Distribution Management and Terminology*.