Development and Evaluation of Information System Security Policies

S.B. Maynard
Email: seanbm@unimelb.edu.au

A.B Ruighaver
Email: anthonie@unimelb.edu.au

Department of Information Systems,

University of Melbourne, Australia

INTRODUCTION

The quality of an organization's security policy has considerable impact on its capacity to prevent serious breaches of its security and to recover from these breaches at minimal cost. The results of surveys conducted over the past 5-10 years have shown organizational interest in security is on the increase and that security measures, including the development of organizational security policies have become more important (James and Coldwell 1993; Ernst and Young 1995; Davis 1996; Kearvell-White 1996; Ernst and Young 1997, Ernst and Young 2002).

While information security policy development has some foundation in the literature, it is uncertain how often the methods described in literature are really implemented in an organizational setting. The cost and complexity of the policy development process has lead to the construction of extensive life cycle models, which are really only relevant to those organization that need, and can afford, to develop and maintain a high-security Information Systems environment. Little is found in literature about how organizations with lower security profiles develop security policies, how these policies are documented, what factors contribute to policy effectiveness and how policy effectiveness is determined.

What is known is that in many organizations security policies simply are not developed at all, or end up on the shelf. To rectify this situation a more pragmatic approach to the development of security policies is needed. In addition, a better foundation to evaluate the quality of the process used to generate a security plan, and to evaluate the quality of the security plan itself is required. Currently, security evaluation research focuses on the evaluation of how well information systems are secured in relation to a security policy statement or security plan. Again little of the literature in this area seems relevant to organizations that do not have a high priority for security.

In this chapter we identify potential problems in current security policy development practice, and offer suggestions about how these problems may be addressed. We will emphasize that organizations should not see the policy as the only artefact of the development process. We propose that they should concentrate on how the security policy is developed and use the development process as a tool, not simply to develop the policy, but to achieve additional benefits for the organization as well. By defining for the business, the benefits of using a policy development process, rather than just a policy; it will be more likely that an increase in management support for security policy development will occur. Emphasizing that there is no need to develop a comprehensive security policy in one hit and that, by empowering employees

in the policy development process, it may be possible to reduce costs through changing how awareness and compliance are dealt with offers a major selling point.

THE NEED TO REDEFINE INFORMATION SECURITY POLICY

As more frequent security incidents are experienced, the need for organizations to become more involved with securing and actively protecting their information from malicious and non-malicious acts is apparent (Jung, Han and Lee 2001; Liebmann 2001). Consequently, the importance of having a well-defined strategic security policy document should be becoming evident to many organizations. The process of developing a strategic security policy forces a company to identify risks to their information and to plan for the possibility that its information system is a viable point of attack, either from internal or external sources. Failure to do this adequately can lead to a number of problems for organizations. For example, there are a number of anecdotes showing that employees who behave inappropriately cannot be dismissed, as no security policy existed stating their behaviour was inappropriate, even though it was damaging to the organization (Leinfuss 1996; Robinson 1997).

The risks to organizational information are often underrated by organizations that do not realise the importance of protecting their information. They underestimate how costly, financially or to the image of the organization, it would be if the information fell into competitors' hands, or was misused. It is an unfortunate fact that securing an organization's information is not considered a core business objective by most organizations. As a result, some organizations are unwilling to make the hard decisions required to protect their information. Fortunately there are signs that this is changing; the impact of global security issues and events has begun to have the effect of increasing the awareness of security from a managerial perspective.

The interest and awareness of organizations with regard to securing their information assets has increased steadily over the last decade (James and Coldwell 1993; Ernst and Young 1995; Davis 1996; Kearvell-White 1996; Ernst and Young 2002). In particular, the development of organizational security policies has become more important. An Ernst and Young (1998) survey found that 56% of organizations had security policies in place. Unfortunately, many of these policies are not audited or maintained and only 64% of those organizations having a policy monitored compliance with the policy (Ernst and Young 1998). It is clear that the uptake of policy development is on the increase within organizations, but policy maintenance and policy compliance in some organizations, remain problem issues.

A number of organizational issues need to be addressed to improve information security. Any improvement to an organization's security policies will result in a tangible improvement in the security of information and systems, and may, in turn, improve customer and employee confidence about the safety of organizational information. The addition of practical knowledge to the theoretical background and research will improve research and commercial practice in information system security policy development.

WHAT IS A STRATEGIC INFORMATION SECURITY POLICY

There are several definitions of information systems security policy. Olson and Abrams (1995) define a security policy as "the set of laws, rules and practices that regulate how an organization manages, protects and distributes resources to achieve specified security policy objectives. These laws, rules and practices must identify criteria for according individuals authority, and may

specify conditions under which individuals are permitted to exercise their authority." This definition is similar to those given by other researchers (Kokalakis and Kiountouzis 2000, Henderson 1996, Robinson 1997). A security policy is thus attempting to protect an asset, either physical or information based, from malicious or accidental damage. By establishing a recovery plan within a policy, the organization is prepared for the worst possible situation.

What many of these definitions fail to do is to differentiate between the different types of security policy within an organization. The term "security policy" means different things to different people. Some employees would define it as the "Acceptable Use Policy", or the "Internet and Mail Policy", others would define it as the "Information Security Statement" or the "Information Security Policy". There are vast differences between these types of policies. The "Acceptable Use" type policies, known as task, process or system specific policies contain system or task specific details, whereas the organizational type policies contain the strategic policy statements for the organization.

Often an organization will develop a hierarchy of policy documents to deal with "security policy". The hierarchy may have documents like an "Information Security Policy" or "Information Policy" at the top and will have documents like "Email Usage" or "Internet Use Policy" at the lower levels of the hierarchy. The strategic policy statements in such a case will be within the top one or two levels of the hierarchy. Figure 1 shows a hierarchy of security policy which is typical of the policy structure within a large organization.

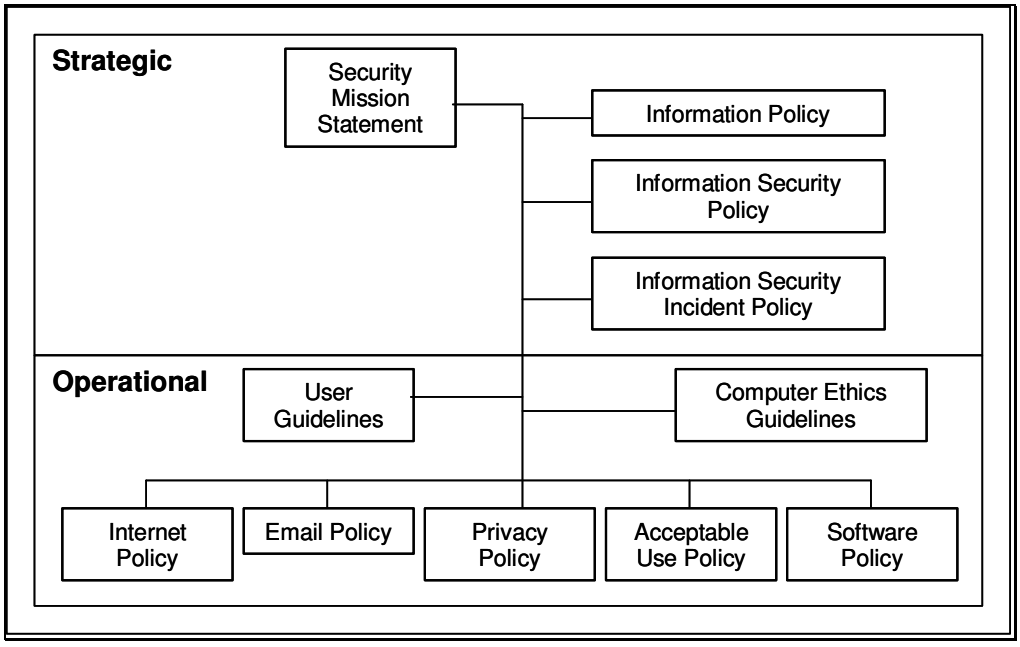

Figure 1 : A typical set of security policy documents

This research deals exclusively with those policies designed at a strategic level to protect the organizations information assets.

SECURITY POLICY DEVELOPMENT PROCESSES

There are many methods discussed in the literature about how to write a security policy. These methods can be split into several groups. The first group uses a set of pre-written authoritative

policy statements that are used to produce a workable policy. There are several companies specialising in selling these types of tools to organizations (Pentasafe Security Technologies[1] 2001, Solsource 1998). The writing of the policy involves determining the area of risk within the organization and then selecting from a number of pre-written statements about that particular area. This is done in a similar manner to piecing together a jigsaw. Often a sample policy is shown to give some sort of idea what a completed policy should look like. This method is a fairly inexpensive way an organization can go about producing a policy. All they need to do is to purchase a document outlining the policy statements with directions on how to use them. Alternatively a company representative can be hired to tailor the policy statements for the organization, producing a tailored security policy. These types of policy efforts are directed to what we would call "Operational Security Policies", and would be used for the development of those policies in the bottom half of Figure 1.

The second group defines process-oriented methods of security policy development that could be used to generate strategic or operational type policies. This method involves the development, implementation and on going maintenance of the security policy within the organization. The security policy produced is tailored specifically for the organization and will probably be useless to any other organization. In general, these methods either semi formally or formally imply a process of security policy development, which never really finishes as it has an iterative nature. The semi formal security policy development processes include those from Bayuk 1996, Control Data 1999, Woodward 2000, DTI 1999, Computer Technology Research Corporation 1998 and the State of Oregon 1998. An example of such a process is shown in Figure 2.

[1] Formally the company was called Baseline Software

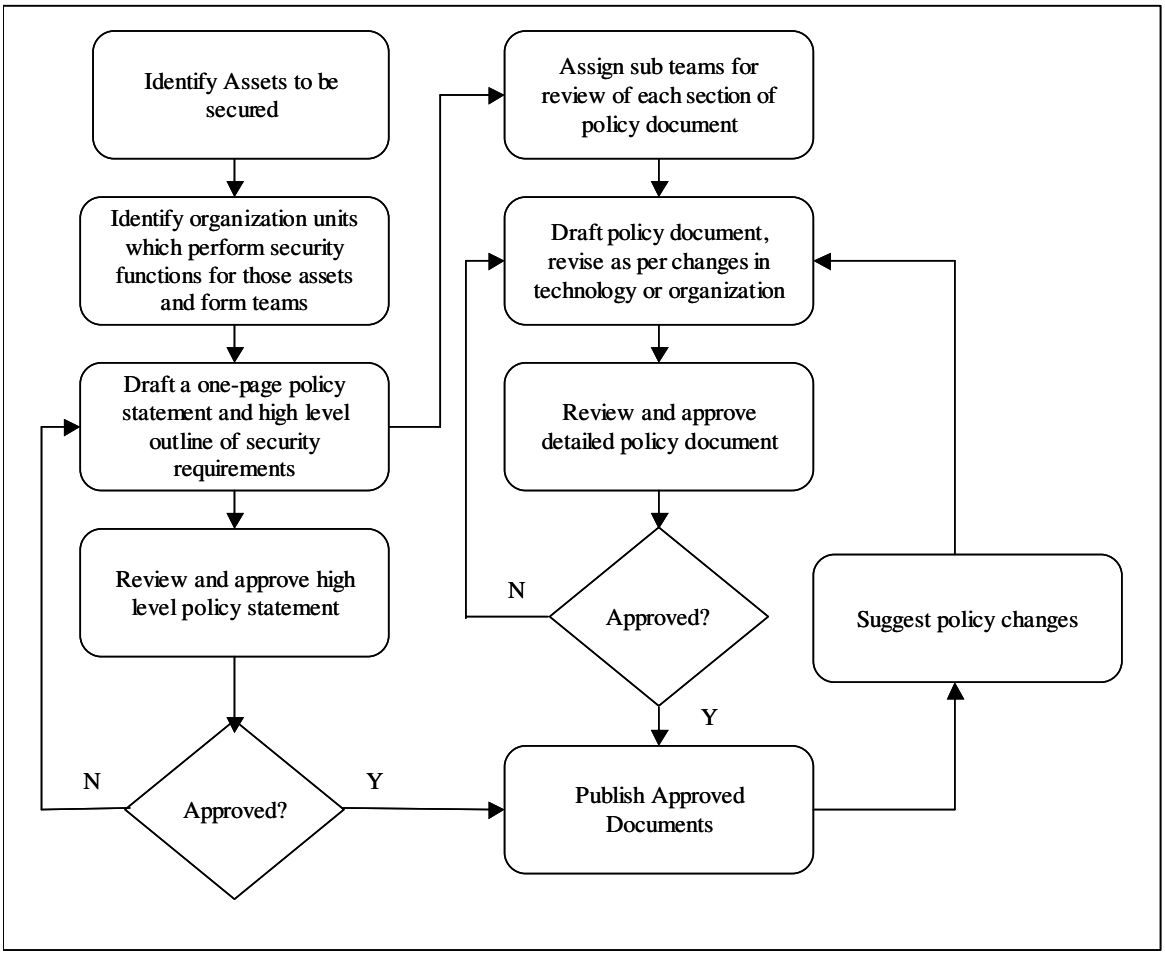

Figure 2. A Process of Policy Development Bayuk (1996)

Essentially the process starts with the identification of what to secure and progresses, through a series of prototype documents, to producing a draft policy. Then the policy is approved and published; from this point the process repeats itself as the policy is continuously updated. Whilst this method describes the process of development, it has little guidance as to what contents should be included in the policy. It states that a one page policy statement for each asset and a high level outline needs to be produced, but doesn't guide what should be included in this documentation.

The more formalised process-oriented methods are more difficult to find and have a formal focus on the security policy development lifecycle. The main example of this type of method is the PFIRES model for e-commerce security policy development as shown in Figure 3. (Rees and Bandyopadhyay 2000, Anderson Consulting 1999). This method mimics a combination the System Development Lifecycle approach and the new product development lifecycle. It has 4 phases:

1) Assess
    a) Policy Assessment
    b) Risk Assessment
2) Plan

a) Policy Development

b) Requirements Definition

3) Deliver

a) Controls Definition

b) Controls Implementation

4) Operate

a) Monitor Operations

b) Review Trends and Manage Events

The important feature of this model is its formalised feedback loop that enables continual feedback to any phase of the development lifecycle.

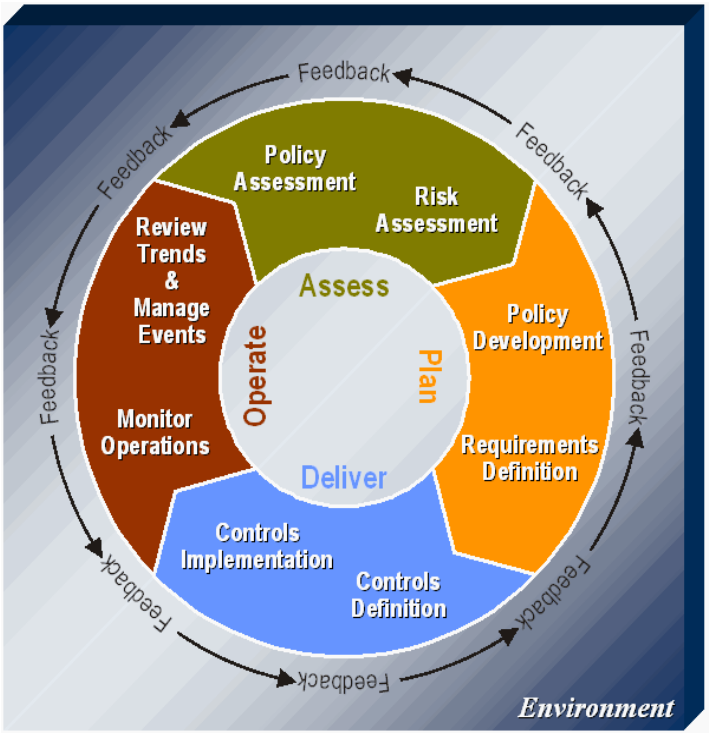

Figure 3: PFIRES Life Cycle Model (Rees and Bandyopadhyay 2000)

PROBLEMS IN SECURITY POLICY DEVELOPMENT

There are several areas of concern for organizations to address as they carry out the development of an information security policy. In the following sections, the issues shown below will be discussed.

1) The cost of policy development

2) Strategic security policy is not a core business objective

3) Support of the influence of the policy lifecycle on the policy development

4) Enforcement of security policies

5) Documentation of security policy development
6) Security Policy Awareness
7) The lack of guidance as to how to develop security policy contents
8) No link between risks and policy statements

The cost of policy development

An issue rarely discussed in research is the cost of information security policy development. As with any organizational expenditure, the cost of implementing an information security policy will affect the bottom line. Through the use of a policy, an organization may save money by balancing the risks of not having a policy, and benefits that the policy provides. For some organizations the cost of policy development would outweigh the risks and therefore that organization may decide not to implement a policy. For other organizations, though, the policy may provide leverage for the implementation of security measures and may prevent major loss of information assets.

Consequently, before strategic information security policies are developed, clear benefits must be perceived by the organization. As the importance of information for an organization's core business activities increases, so does the benefits of protecting that information. At a certain point, the benefits of insuring the information through the use of a policy will outweigh any costs incurred by the development and implementation of the policy.

The role of reuse in security policy development must also be addressed. It is often the case that much of previous security policies can be reused in updated policies. Furthermore the cost of security can be reduced through more thorough involvement of organizational personnel. For strategic based policies if middle to upper management involvement was included in development then the ownership of the policy and therefore the awareness of security and the security policy would be given to these personnel. Likewise for operational policies user level employees could be made to feel ownership and responsibility towards security. If this was done the cost of security enforcement and compliance monitoring may be reduced as the drivers behind security would be the employees, rather than IT management; essentially this is a culture building exercise.

Strategic security policy is not a core business objective

As information and information processing capabilities of organizations are generally critical for the functioning of the organization, it important that these be protected through physical measures and via organizational policies. Organizations need to realise the consequences if suddenly their information was not available, was corrupted in some manner, or was handed to their competitors. Swanson and Guttman (1996) therefore suggest that these resources should be protected like other important organizational assets: by having adequate policies and procedures. Unfortunately, as many organizations do not recognise the value of their information, security of that information tends not to be regarded as critical to the business. Woodward (2000) suggests that organizations must determine how important their information assets are to the functioning of the organization so that they are able to make this link.

The greatest obstacle for organizations in addressing security concerns is the lack of support given from senior management (Ernst and Young 1998)[2]. As security does not form part of the core business objectives, some organizations rather put resources into what they think are more profitable areas. Furthermore, in some organizations where state of the art security exists it is not used effectively, or is not supported with effective procedures and policies. "By itself installation of hardware and software for security can not protect an organization's assets" (Henderson 1996). Having these physical aspects of security covered does not mean that employees, or outsiders, will not knowingly or unknowingly compromise these security efforts. Others agree that any physical security measures implemented will be less effective without policies and procedures designed to protect the organization's information assets (Swanson and Guttman 1996, Guttman and Bagwill 1999, Bayuk 1996, Control Data 1999). Adequate security is having quality security policies being defined by appropriate people in an organization that go hand in hand with technologies to protect the organization's information assets. An analogy here can be drawn between the security policy and insurance policies that organizations purchase. The security policy is an attempt to provide insurance for the organization's information.

This leads to the question "who should develop security policy?" This seems to best be answered by stating that no single individual should develop the policy (State of Oregon 1998, Henderson 1996). Having multiple stakeholders involved in the policy development tends to reduce the impact of implementation of the policy and allows for multiple perspectives to be met within the policy. It is also argued that those people developing policy statements should be senior in the organization, and should come from every functional area. Further, it is argued that it is extremely important to have the commitment of all senior executives throughout the organization as the policy may change the way in which things are done within the organization, it must be seen as being a directive from above (State of Oregon 1998). Without this, it is possible that employees will think the policy is unimportant and will continue as before, possibly continuing to infringe some of the policy principles.

Unfortunately, obtaining senior level commitment does not seem to be occurring in organizations. Warman (1995) states that security policy formation is only being carried out at a low level in organizations, that the requirements of end users are taken into account, but their involvement in the development of the policy is discouraged, and the amount of executive level involvement in the development is minor. This is directly opposite to the views of normative writers on the subject (who state that there should be high management involvement in policy development), which may either suggest that the theory is incorrect or that organizations are ignoring the theory. Warman (1995) observes, "It is interesting therefore to note the contrast between the ideas and theory of security policy that appear to be recognised and accepted, and the actual practice of their implementation within organizations [which does not follow the theory]". Furthermore, it is unlikely that senior staff will want to participate in a security policy development if it is not considered core to the business.

Support of the influence of the policy lifecycle on the policy development

The influence of the policy lifecycle on policy development deals with when and how the policy is updated and whether it is being enforced. In essence this is a policy audit that tests whether

---

[2] 19% of organizations also stated that management support was the greatest obstacle to addressing security concerns (ibid.)

people are complying with the policy, and if the policy needs to be modified to incorporate changes to the information risks faced by the organization.

Some organizations who have a security policy fail to revisit that policy periodically to determine if it is still effective. Several of the development methods discussed previously briefly describe the development of the policy as a process that goes through continual re-development, yet neglect to specify how it is determined what needs to be updated, added or removed from the policy. Consequently, there is little information about how to determine if the information security policy is effective in achieving the aims of development determined by the organization. This may also be caused by the policy having no link between risk and policy statements.

This issue is further clouded by organizations out-sourcing security policy development. Presently there are numerous companies that sell their services as security policy development professionals, or who provide a number of templates to companies on which they can base their policy (for example Solsource 1998). Many companies are blindly using this service without thinking about the consequences. They have no organizational memory dealing with the development of the security policy; rather, they have the end artefact – the policy itself. This does not only occur in the case of out-sourced policy development. Loss of organizational memory regarding security policy can also occur for internally developed policies. Employees may leave the company and the expertise they have developed in creating the security policy is lost to that company if it is not documented.

Enforcement of security policies

Clearly having a security policy alone is not enough. The majority of companies that have clearly stated policies do not enforce them adequately (Robinson 1997). Ernst and Young (1998) report a drop from 74% (in 1997) to 64% (in 1998) in the number of organizations monitoring compliance with policy. This indicates that there may be a problem in organizations allocating resources for the compliance process, or that organizations have a problem in identifying how to monitor compliance. Once again, this may be a result of research not specifying methods of testing whether compliance with a security policy is present within the organization. It is important that a security policy not only exists but also is enforced within the organization; otherwise the organization is leaving itself open to widespread damage from internal and external security breaches. Hence, it is important for organizations to have a strategy of ensuring that the policy is communicated to employees and is enforced.

A possible reason for this inadequacy of enforcement is that many of the security policies developed in organizations are very rich in the information they contain and that it is difficult to enforce something that is not clearly understood. McMillan (1998) suggests that security policies should contain only principles. Many policies developed currently are not principles documents. They attempt to fit everything into the security policy: the justification of importance and specific system instructions and descriptions. The practice of putting it all in the information security policy has a direct link to the manner in which these policies are developed. A useful analogy here is software development. Imagine if all of the documentation for the development of a software product was completed as a part of the program code produced. This seems to be a flawed approach. An improvement to this approach could be the better use of documentation techniques within the development of the policy causing the security policy to become a principles document. Other issues not dealing with the principles of security policy could then be documented elsewhere along with the justification for the policy.

Documentation of security policy development

A major problem is the lack of documentation produced by current information security policy development methods. Documentation of the security policy process is critical to ensure that the policy developed can be justified. Also the documentation of the how and the why of policy development may allow for future redevelopment of the policy allowing organizations to better determine the effectiveness of the policy. Each of the development methods discussed suggests what needs to be done to develop a security policy, but, as nobody mentions the need to document the development process of the policy, many organizations arrive at a security policy (that may or may not be well developed) that seems to its users as having no documented basis. This lack of adequate documentation also hampers the inevitable further development and adaptation of the security policy to a changing environment.

For example, Henderson (1996) discusses the development of security policy through the identification of why the policy is needed, who should develop it, how detailed it should be, and what it should contain. There is no concept of documenting the process, or the policy, to enable ongoing change and management of what should be an evolving document. As a result, if the person(s) who wrote the document leaves the company the document may never be maintained, enforced, or even used.

Security Policy Awareness

The major threats to information that organizations face originate from both unauthorised and authorised users. In an Ernst and Young (1997) survey malicious acts by current employees were reported by 43% of organizations. These acts all resulted in some effect on the information processing capabilities of the organizations involved. However, from these results it is unclear as to why these acts were committed. The fact that employees are causing the information assets of the organization to be affected by their actions is potentially a large problem to many organizations. If information is not safe internally then how does an organization guarantee that its information will be correct and un-adulterated? This problem could be attributed to the general lack of security awareness that is shown by many organization workers.

In the 1998 Ernst and Young survey, 34% of respondents state that employee awareness was the greatest obstacle to addressing security concerns. Traditional approaches to generating security policies tend to generate a policy and then train your personnel to obey the policy. This is not only very costly; it also does not seem to be giving sufficient results within organizations. Thus, it is necessary for the organization to attempt to change cultural values to make clear that security is a key issue and to give employee's clear ownership of security. One way to do this is to have more involvement in security policy development at all levels within the organization to enable staff to see why it is important and to feel part of the process. As awareness in security grows, employees will be better able to identify breaches of security and would be more inclined to report incidents.

Awareness is also affected by organizational change. The development of an information security policy may introduce radical changes to information processes and to the culture of an organization. The marketing of the policy and education about the policy are important in order to help to manage the changes to the organization resulting from policy implementation. Employees should be made aware of why the policy is being implemented, how it will affect them and what the consequences are if they do not follow it (Leinfuss 1996, Control Data 1999).

By involving employees in this manner it is more likely that they will be committed to the policy and will actively participate. Bayuk (1996) states "…policy dictates what must be done to provide an acceptable level of assurance that systems are secure. Awareness process ensures that people know what must be done. To achieve assurance that policy is being followed uniformly throughout the organization, security management must also address how policy is to be realised." The policy in essence should be shown as critically important to the functioning of the organization. Without careful education and marketing of the information security policy it may be regarded as just another "stupid policy".

Security policy awareness needs to be taught in a tailored manner and employees must be taught the values of the assets, the risks and the costs so that they are better able to appreciate the policy and thus comply with it. Unfortunately, the importance of the different risks is seldom mentioned within the security policy. The other issue here is making sure that employees have access to the security policy. There is some anecdotal evidence showing that organization's strategic security policies are treated as confidential documents not to be shared outside the organization, hopefully these documents are available for all employees within the organization.

The lack of guidance as to how to develop security policy contents

As the approaches for security policy development discussed earlier show, there are many authors, who describe in a normative manner how a security policy should be written. It is apparent that each describes the structure of the security policy, but in general, fails to describe the process used to generate the output of the policy development process. It is a standard practice to describe what should be in the policy, but not to back it up with any obvious industry case studies, or examples (Leinfuss 1996; McMillan 1998; Computer Technology Research Corporation 1998; State Of Oregon 1998). This focus means that there is no clear link with what is written in research and what is done in industry. Also, whilst there is evidence of reusing policy statements in the first approach, in the second approach there does not seem to be any attempt to reuse any part of the developed policy in policy updates.

No links between risks and policy statements

In some organizations, depending on the development method chosen, the policy statements developed may not be directly attributed to the risks to the information they are designed to nullify. It is important to be able to have a verifiable link between the risks to information and to the policies aimed to reduce these risks. Unfortunately, with the development methods discussed above there is no link evident. The key to this problem may lie in better documenting the process of information security policy development (this is discussed further in a subsequent section).

WHAT SHOULD BE DONE TO IMPROVE THE SITUATION

From the issues discussed above it is clear why many organizations are struggling to deal with the security policy development process. Perhaps the best place for an organization to start is with the question: What are the benefits to the organization of developing and maintaining an appropriate strategic security policy? Even if improving security is the main objective other objectives could be to increase the awareness of the risks the organization faces, to reduce the cost of security, or allowing the evaluation of the security policy process. From this point it may then be beneficial to use the issues discussed above to generate the answer to this question. This section will outline a number of guidelines as to how organizations may want to proceed to

attempt to address these issues. Many of these may have been touched on in the previous discussion.

Reducing the cost of policy development

The benefits of using a policy development process, rather than just a policy, need to be defined for the business. Reducing costs through changing how awareness and compliance are dealt with by empowering employees in the policy development process may be a selling point. Make use of reuse. Through the documentation of the policy development process meaningful information will be generated that will allow reuse to occur when updates to the policy occur. Clear indications will be present identifying why certain decisions were made about the structure of the policy and about security in the organization. You do not need to reinvent the wheel.

Making strategic security policy a core business objective

If the focus the policy development process is on the core business issues it is more likely to get management support. Once an initial policy is developed then look at the most important core issue and begin a constant process of enhancing the security policies. There is no need to develop a comprehensive security policy in one hit. Realise that the security policy will be in need of constant change and address that change using the core issues and develop many iterations of the policy by focusing on these issues. This focus on the core issues should attract interest of all relevant stakeholders, including management.

Supporting the policy lifecycle

In our view security should be exclusively developed within the organization. If necessary outside consultants can be asked for advice, but the organizational knowledge about the development must be kept within the organization. Also, attempt to avoid losing organizational memory when people move on from their current positions by using the development process wisely to document decisions. This may be a knowledge management issue. Finally, do not attempt to develop the ultimate security policy in the first instance. This will take too long and may end any support the process had at an organizational level. Rather, as stated above, use strategic issues as a guide as to what to do first.

Improving the Enforcement of security policies

Organizations should use the KISS principle (Keep It Simple Stupid). Only put policy statements in the security policy if they are understandable by all employees. Keep the security policy a principles document that is uncluttered by unnecessary information. Use other documents to store other information that doesn't belong in the policy. As for Security Policy Awareness, involve any people who are likely to be influenced by the policy in the development process as this will likely help you enforce the policies in the long term. As awareness of the policy increases employee self enforcement of the policy should also increase.

Better documentation of security policy development

Many of the problems dealing with organizational memory may be relieved if organizations develop a self documenting process of security policy development. They can use this documentation to explain the reasoning behind the development of the security policy. This

documentation can also be used for evaluation of the current policy and for the further documentation of resulting policies.

Increasing Security Policy Awareness

Organizations may wish to change the attitudes of their employee's by encouraging them to play a role in the policy development. Giving them ownership and teaching them an understanding of the importance of security within the organization is paramount. The empowerment of employees with regard to security will result in a cultural shift that will mean that part of every employee's job will be to ensure that security is not compromised. This may in turn, reduce costs of awareness training and enforcement. In a similar vein, organizations should promote the successes of the policy, rather than focusing on the security breaches that occur. This will enable the organization to move forward, and will show the policy as a "good thing" and will further promote it awareness.

Improving guidance as to how to develop a security policy

There are plenty of good examples of security policies generally available publicly via the internet or within organizations. However, having the policy artefact is only one of the benefits of the process of strategic security policy development. Organizations should concentrate on how the security policy is developed and use the development process as a tool, not only to develop a policy, but to identify additional benefits for the organization. The process itself should document how the policy was developed, what decisions are made, which policy statements are derived in answer to what risks.

Linking risks and policy statements

Most security policies lack the link between risks and policy statements. In many instances it is possible to easily transfer policies between organizations and they would be appropriate for the new organization. This indicates that the policy statement is not tailored enough to the risks the organization. The above documentation process could be used to document the process used to identify the risks important to the organization. This documentation can also be used to link risks to policy statements so that a clear understanding can be made. This is especially important in those organizations that do not perform a traditional risk assessment.

EVALUATING POLICY DEVELOPMENT AND OUTCOMES

The general approach for testing security in organizations is to conduct a security audit. A security audit essentially looks at the implementation of a security policy within the organization. Some facets of the security audit may look at how risks have changed and hence may provide an indication that the security policy needs to be updated. This should be part of the lifecycle of the security policy as discussed before. However, the lifecycle will in general, only look at the coverage of the security policy, and will not otherwise evaluate the quality of its contents.

In the following sections we will look at the evaluation of the quality of policy and procedures. First we look at the methods of evaluation used to ensure the quality of Information Systems products from a security perspective. We will then look at the methods of quality assurance used in information systems development. Finally we suggest how these approaches can be used to improve the quality of information systems security policies.

Security Evaluation of Information Systems

The first concept of security evaluation originates in the US Department of Defence with the Trusted Computer System Evaluation Criteria (TCSEC) or the Orange Book published in 1985 (US Department of Defence 1985). This was the baseline for security evaluation certainly in "high risk" government institutions, but also in some commercial situations. Since the publication of these criteria, significant changes to the computing industry have taken place and many attempts at developing a standard form for security evaluation have been made.

In 1991 the European standard for evaluation: Information Technology Security Evaluation Criteria (ITSEC) was developed by France, the UK, the Netherlands and Germany (Nash, Brewer et al. 1991). Also in 1991, ISO/SC27 WG3 began work on evaluation criteria to be used in quality assurance of products. The Canadian evaluation effort began in 1993 with the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) (CSSC 1993) as did the new US standard, aimed at updating the TCSEC standard (NIST/NSA 1993). This effort was shelved, as researchers started a cooperative effort between the USA, Canada, France, Germany, the Netherlands and the UK (Overbeek 1995) to develop a set of Common Criteria for Information Technology Security Evaluation (CC).

The CC approach attempts to combine the best aspects of both TCSEC and ITSEC to try to ease the mutual recognition of evaluation results between nations. It is an attempt at a set of "harmonised" evaluation criteria whose aim is to be accepted globally, enabling a single evaluation of a product, rather than one for each region. These documents all have several things in common. Firstly they not only focus on the evaluation of finished products, but also on the development process, to attempt to see if systems are secure. Further, these product evaluation methods tend to have a military focus. Lipner (1991) suggests that there should be a distinction made between systems that have a military focus verses those that are commercially oriented.

The problem with each of these methods is their narrow focus on the product and its development process, rather than on the whole environment in which that product will be implemented. So even if the product has a high security standard, it may be implemented in an organization with a security policy that is substandard, incorrectly implemented, or even missing.

From these initial efforts a number of standards have now been produced that focus on the organizational implementation of security rather than on products. These standards include BS 7799, AS/NZS 17799:2001, ISO 17799). Unfortunately, the adherence and uptake of these standards in industry is questionable. For instance in the UK where the BS 7799 standard has been in use in its revised form since 1999, many organizations, whilst being aware of the standard, are unable to state what it covers. "Whilst BS 7799 has become the international standard of security, only 15% of people responsible for IT security in the UK are aware of its contents" (DTI 2002). Whilst there is no information regarding similar experiences with the ISO 17799 or AS/NZS 17799:2001 standards, anecdotal evidence seems to suggest that the findings of the UK survey would be comparable internationally.

Documentation of the Development Process

The process of the development of security policies can generally be described as a process of identifying and documenting possible points of failure in the organization's technology infrastructure as well as in the protection of this infrastructure. Before a successful evaluation of a security policy can take place, it is likely that a new standard regarding the documentation of

the development process, necessary for such an evaluation, will have to be developed. The IS product security evaluation efforts explained in the last section attempt to enforce this from a product perspective. Not only do they evaluate the end product, they force developers to follow standards in the development process to provide documentation on which to base the evaluation.

In comparing the security policy development process occurring in many organizations to the current practice in software development, the documentation produced in security policy development is negligible. In fact, in real terms, documentation of security policy development is in the 1970's when compared to software development efforts. From the software development perspective, the development documentation is quite evolved and, as a result, the failure of many projects has been avoided through the use of the prior development documentation. In a similar manner, providing the product security evaluation with the required documentation may enable the evaluation to identify possible improvements in the policy development process, and to the security policy artefact.

Most authors, who describe, in a normative manner, how a security policy should be written never indicate the importance of documentation within security policy development. Authors focus on the need for a policy, making sure it can be enforced, training users, and making sure that it has management support (Henderson 1996; Computer Technology Research Corporation 1998). Each suggests what needs to be done, in turn, in order to develop a security policy. But, as nobody mentions the need to document the development process of the policy, many organizations get a security policy (that may or may not be well developed) that seems to its users as having no documented basis. This lack of adequate documentation also hampers the inevitable further development and adaptation of the security policy to a changing environment.

The out-sourcing of security policy development by some organizations further complicates this situation. Presently there are numerous companies that either sell their services as security policy development professionals, or who provide a number of templates to companies on which they can base their policy (for example Solsource 1998). Many companies are blindly using this service without thinking about the consequences: having no organizational memory dealing with the development of the security policy. Rather, they have the end artefact – the policy itself. This does not only occur in the case of out-sourced policy development. Loss of the organizational memory regarding security policy can also occur for internally developed policies. Employees may leave the company and the expertise they have developed in creating the security policy is lost to that company if it is not documented elsewhere.

Enabling the Evaluation of Security Policies

The previous section suggests that the development of a security policy should be more akin to the development of an information system, or to the development of products being evaluated by one of the product evaluation methods discussed. This would produce the documentation required for an evaluation process to be conducted at a security policy level within the organization. At present with the only artefact of security policy development being the policy, it is the only thing that can be evaluated.

The development of an information system progresses through several distinct phases from analysing the problem through to the implementation of the system. Throughout this process each step is documented through a series of deliverables that range from a feasibility study, through to training manuals and system documentation. In the development of a security policy this self-documentation process does not occur. Nowhere in a security policy is it made explicit

how the document was created, who was consulted in its production or how the policy was implemented. Nor is there any documentation of political problems that may have occurred during the implementation of the policy, or of how to train people about the policy.

McMillan (1998) suggests that security policies should only contain principles. Many policies developed currently attempt to fit everything into the security policy: the justification of importance and specific system instructions and descriptions. With the use of documentation techniques within the development of the policy, a security policy would become a principles document. Other issues not dealing with the principles of security policy would be documented elsewhere along with the justification for the policy.

Currently, a security policy evaluation procedure would concentrate on the policy its self without considering other issues in the organization that may have contributed to the development of the policy. This has potentially dangerous consequences. For instance, there may be political pressures to implement a policy quickly and the policy is, thus, forced upon users without any consultation. As a result users need to remember three different passwords that are forcibly changed every week. This may in fact decrease security in the organization, as several of those users would probably write their passwords down to remember them! Through having documentation available, in addition to the security policy, detailing the methods used in policy development, the evaluation focus on the policy is at a greater depth, rather than superficially evaluating the end product. For instance, rather than concentrating only on whether the policy has been implemented in a particular area, the focus can also look at how that area was developed within the policy. Documentary evidence could be evaluated to determine if the policy adequately covers all issues identified within development without watering any of them down.

The methods used for evaluating products (ITSEC etc) may have useful parallels when it comes to the development of an evaluation method for security policy. Likewise the standards for security (BS 7799, ISO 17799, AS/NZ 17799) may also have a role to play in improving the development of strategic security policy. The target of both of these things is to protect confidentiality, integrity and availability of the system. They are both also stimuli that enables companies to comply with a set security standard.

These aims are similar to what is required of a security policy evaluation method. Security policies vary greatly depending on the context of the organization and one would think that their development would also vary. Some commonality between policies would exist, even as target areas digress. Unlike product evaluation however, many criteria in security policy evaluation will be of a subjective nature. This is because of the subjective nature of developing a policy and of the environment in which the policy is implemented.

SUMMARY

This chapter suggests that in general terms the process of strategic information security policy development must be revisited. We suggest that there is no clear link between research and industry practice for security policy development, and that current development practices portrayed in research do not adequately describe the development process. Furthermore, we argue that in most security policies the link between risks and policy statements is unclear and that before the effectiveness of an information security policy can be tested a new standard regarding the documentation of the development process, necessary for such an evaluation, will have to be developed.

An initial approach to improving the security policy development process may be to enforce similar standards to those used in information systems development. This will focus those developing the security policy, not only on the content of the policy, but also on the documentation of why that content is there and for what reasons. The security policy development then incorporates a security documentation process. The ultimate responsibility of the appropriateness and usefulness of the policy lies with those who have designed it. If they can show documentation about the design that elaborates on the policy then policy developers can show the origins of the policy are valid.

We have identified areas where similarities exist between security policy evaluation and the system security evaluation processes currently being used. The methods of security product evaluation not only all attempt to evaluate the finished product, but all look at the complete development process. This not only makes the evaluation process more comprehensive, but also aids in the quality assurance of the product. If this can also be applied to the development of security policy then it is expected that the quality of policies and their implementation will improve.

Subsequently, we argue that the current practice of security policy development is inadequate for a number of reasons. First, security policy development tends to produce only the artefact – the security policy, rather than documenting the process of development. Second, security policy research suggests that a number of steps be taken in policy development but survey analysis suggests that organizations are not applying this to their policy development. We suggest that in a similar manner to modern software development processes, that a prototyping approach may often be better suited to the waterfall approach for developing security policy.

Whilst we argue that strategic information security policy should be a core business objective, we recognise that for any particular organization the extensiveness of this policy will vary. The resources an organization allocates to develop and implement a strategic information security policy will, like all organizational decisions, really depend on economical issues. For many small to medium sized organizations, the cost of security policy development and maintenance is excessive. Hence a small policy concentrating on the current key issues in information systems security may be more appropriate. However, the importance being placed by many organizations on Electronic Commerce and other leading edge technologies is likely to tip the scales towards having a more comprehensive strategic information security policy, as the likelihood of severe losses will increase dramatically.

BIBLIOGRAPHY

Anderson Consulting. (1999). *Policy Framework for Interpreting Risk in eCommerce Security*. Retrieved September, 2002, from the World Wide Web: https://www.cerias.purdue.edu/techreports-ssl/public/pfires/

Bayuk, J., L. (1996). *Security Through Process Management*. Morristown, NJ: Price Waterhouse.

Computer Technology Research Corporation. (1998). *Security Policy : Key to Success*.

Control Data. (1999). *Why Security Policies Fail*. Retrieved, from the World Wide Web: http://www.securityfocus.com/data/library/Why_Security_Policies_Fail.pdf

CSSC. (1993). *Canadian Trusted Computer Product Evaluation Criteria (CTCPEC): Version 3.0*: CCSC, CSE.

Davis, C. E. (1996). Perceived Threats to Today's Accounting Information Systems: A Survey of CISA's. *IS Audit and Control Journal, 3*, 38-41.

DTI. (1999). *The Business Managers Guide to Information Security*. Department of Trade and Industry, UK. Retrieved March, 2000, from the World Wide Web: http://www.dti.gov.uk/cii/datasecurity/businessmanagersguide/index.shtml

DTI. (2002). *Information Security Breaches Survey*. Department of Trade and Industry, UK. Retrieved January, 2002, from the World Wide Web: http://www.dti.gov.uk/cii/datasecurity/businessmanagersguide/index.shtml

Ernst and Young. (1995). The Ernst and Young International Information Security Survey 1995. *Information Management and Computer Security, 4*(4), 26-33.

Ernst and Young. (1997). *5th Annual Information Security Survey*: Ernst and Young.

Ernst and Young. (1998). *The Ernst and Young International Information Security Survey 1998*: Ernst and Young,

Ernst and Young. (2002). *The Ernst and Young International Information Security Survey*: Ernst and Young,

Guttman, B., & Bagwill, R. (1999). *Internet Security Policy: A Technical Guide*: NIST.

Henderson, S. (1996). The Information Systems Security Policy Statement. *EDPACS - EDP Audit, Control and Security Newsletter, 23*(12), 9-15.

James, H., & Coldwell, R. A. (1993). Corporate Security: An Australian Ostrich. *Information Management and Computer Security, 1*(4), 10-12.

Jung, B., Han, I., & Lee, S. (2001). Security threats to Internet: A Korean multi-industry investigation. *Information & Management*.

Kearvell-White, B. (1996). National (UK) Computer Security Survey 1996. *Information Management and Computer Security, 4*(3), 3-17.

Kokolakis, S. A., & Kiountouzis, E. A. (2000). Achieving interoperability in a multiple-security policies environment. *Computers & Security, 19*(3), 267-281.

Leinfuss, E. (1996). Policy over Policing. *Infoworld, 18*(34), 55.

Liebermann, L. (2001). The Enemy Within. *Communications News*.

Lipner, S. (1991). *Criteria, Evaluation & the International Environment: Where we are, Where we Have Been and Where are we Going.* Paper presented at the IFIP TC11 7th International Conference on Information Security: Creating Confidence in Information Processing.

McMillan, R. (1998). *Site Security Policy Development* [WWW Page]. Retrieved 16 Aug 1998, from the World Wide Web: http://secinf.net/info/policy/AusCERT.html

Nash, M., Brewer, D., Chorley, B., Lampard, R., & Williams, F. (1991). *Security Criteria Harmonisation: The Information Technology Security Evaluation Criteria.* Paper presented at the IFIP TC11 7th Conference on Information Security: Creating Confidence in Information Processing.

NIST/NSA. (1993). *Federal Criteria for Information Technology Security (FC), Draft 1*:

NIST/NSA.

Olson, I. M., & Abrams, M. D. (1995). Information Security Policy. In M. D. Abrams & S. Jajodia & H. J. Podell (Eds.), *Information Security an Integrated Collection of Essays* (pp. 160-169). Los Alamitos, California: IEEE Computer Society Press.

Overbeek, P. L. (1995). Common Criteria for IT Security Evaluation - Update Report. In J. H. P. Eloff & S. Von Solms, H (Eds.), *Information Security the Next Decade: Proceedings of the IFIP TC11 eleventh international conference on information security* (pp. 41-49).

Pentasafe Security Technologies. (2001). *Security Policy*. Retrieved May 1, 2001, from the World Wide Web: http://www.pentasafe.com/products/policyoverview.htm

Rees, J., & Bandyopadhyay, S. (2000, August 10-13th, 2000). *A Life Cycle Approach to Information Security Policy for Electronic Commerce.* Paper presented at the Proceedings from the Association for Information Systems 2000 Americas Conference on Information Systems (AMCIS 2000), Long Beach, California.

Robinson, T. (1997). Business at Risk. *Software Magazine, 17*(10), 88-91.

Solsource. (1998). *Corporate Security Policy*. Solsource. Retrieved 27 Nov 1998, from the World Wide Web: http://www.solsource.com/corporatesecurity.html

State Of Oregon. (1998). *Guideline for Developing an Agency Information Systems Security Policy* [WWW PAge]. Retrieved 20 Feb 1998, from the World Wide Web: http://www.state.or.us/IRMD/guidelin/secpol.htm

Swanson, M., & Guttman, B. (1996). *Generally Accpted Principles and Practices for Securing Information Technology Systems*: NIST.

US Department of Defence. (1995). *DOD - Trusted Computer System Evaluation Criteria* [WWW Page]. US Department of Defense. Retrieved 16 Aug 1998, from the World Wide Web: http://www.telstra.com.au/pub/docs/security/orange-book.txt

Warman, A. R. (1995). Developing Policies, Procedures and Information Security Systems. In J. H. P. Eloff & S. Von Solms, H (Eds.), *Information Security the Next Decade: Proceedings of the IFIP TC11 eleventh international conference on information security* (pp. 464-476).

Woodward, D. (2000). *Security Policy Management in the Internet Age*. Retrieved 27 September, 2000, from the World Wide Web: http://www.itsecurity.com/papers/wickpol.htm