An Analysis of IS Security Policy Evaluation

Sean Maynard
Tobias Ruighaver

Department of Information Systems
University of Melbourne
Australia
s.maynard@dis.unimelb.edu.au
t.ruighaver@dis.unimelb.edu.au

Abstract

Information System security evaluation research usually focuses on the evaluation of how well information systems are secured in relation to a security policy statement or security plan. Most studies concentrate on standards of security measurement such as the "orange book", or the European standard (ITSEC). Little research however, concentrates on the manner in which security plans (or policies) are developed, and none, to the author's knowledge, attempt to evaluate the process of generating a security plan, or to evaluate the security plans themselves. This paper is work in progress that discusses the security policy evaluation process.

Keywords

Information System Security, IS Evaluation, Evaluation, IS Policy

INTRODUCTION

The quality of an organisation'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 organisational interest in security is on the increase and that security measures, including the development of organisational security policies have become more important (James and Coldwell 1993; Ernst and Young 1995; Davis 1996; Kearvell-White 1996; Ernst and Young 1997).

The development of a security policy helps an organisation to plan, protect and prosecute. The security policy forces a company to plan for the possibility that their information system is a viable point of attack, either internally or externally by people, or through a natural disaster. By planning for the possibility of an attack and identifying where an attack may occur, the organisation is enforcing some protection of its information systems. The policy development process will identify possible problem areas that are acted on upon the policy's implementation. The policy identifies those who have the responsibility of maintaining and enforcing the different security measures. Further, it makes explicit the responsibilities of users and allows the organisation to prevent some of the problems that would occur without an enforced policy. Research is full of anecdotes where employees have behaved inappropriately but have not been dismissed because no policy stating that their behaviour in that company was inappropriate exists (Leinfuss 1996; Robinson 1997).

Although a poorly designed security policy will significantly reduce the effectiveness of an organisation's security measures, there is, to the author's knowledge, no research where security policy has been the target of evaluation from either the development or use

perspectives. Research has instead focused on the evaluation of a particular company's systems to determine if they are secure, usually without reference to the security policy that the company has developed. Such studies often focus on the evaluation of whether hardware, software and personnel can be considered secure. The premise used in those situations is that, when the company has a security policy, testing the security of the company's systems will, by inference, also evaluate their security policy. This does not, however, take into account the problems involved with the development and implementation of the security policy, which in turn may mean that aspects of the security policy have not been implemented to their full extent.

The question to be asked, therefore, is how one should evaluate the security policy of an organisation. Is it sufficient to only evaluate the end product, or should one also evaluate the process used to produce the security policy. To provide an initial answer to this question, this paper investigates whether there are any similarities between evaluating the security policy (the input to the security process) and evaluating the systems, people and software (the aim of security). It also discusses the evaluation of security policies in relation to traditional system security evaluation processes. This work is the initial stage in determining the issues that influence the development, implementation, ongoing use and evaluation of security policies within organizations.

INFORMATION SYSTEMS SECURITY POLICY

Information security can be defined as the 'measures necessary to safeguard information from unauthorised, accidental, intentional, or malicious modification, destruction or disclosure'. (State Of Oregon 1998).

In general terms, a security policy aids in the protection of the assets of the organisation, including physical assets, as well as information and knowledge that is pertinent to the organisation's operation. Often, people do not realise the importance of protecting their information. They underestimate how costly it would be if it fell into competitors' hands or was misused. In some instances the loss of information may force an organisation into bankruptcy. Surveys have shown that many organisations do not have plans in place to handle emergency situations, such as the malicious destruction of data (Ernst and Young 1995; Ernst and Young 1997). In the case of disaster, many organisations do not have the documentation or procedures in place to effectively cope with the situation.

An Information Systems Security Policy is a document, or set of documents, detailing the responsibilities of all employees in relation to specified Information Systems or Organisational Resources. It sets out the rights and expectations of users and also establishes 'written guidelines' to protect the information and resources within the organisation from intentional or accidental damage (Henderson 1996). It states what cannot, and should not be done as well as recovery plans in instances of policy breaches. Information systems security policy is defined by (Olson and Abrams 1995) as "The set of laws, rules and practices that regulate how assets including sensitive information are managed, protected and distributed within a user organization".

Ultimately a policy exists to "prevent the loss of an asset or its value" (McMillan 1998). It attempts to prevent an asset, either physical or information based, from malicious or accidental damage. By establishing a recovery plan within a policy, the organisation is prepared for the worst possible situation.

The security policy should state the consequences of breaking any part of the policy. If employees or outsiders break the policy then the company has clearly stated what actions they

will take (usually in legal terms). For those internal to the company that may mean losing their jobs, as well as being dealt with in the same manner as those outside the company (through the legal system).

Every company should have a security policy: a set of guidelines that instruct management and employees how to provide a secure work environment. These guidelines also state the acceptable use of the company's computers. But, having a security policy is not enough. The bulk of companies that have clearly stated policies do not adequately enforce them (Robinson 1997). It is important that a security policy both does exist, and is enforced within the organisation. Otherwise the organisation is leaving itself open to widespread damage from internal and external security breaches.

Many organisations are only recently, and slowly, realising the importance of information within their organisation and, as a consequence, are coming to the realisation of the need to have a policy to protect it. Unfortunately this area is still in its early stages of development and as a consequence a lot of literature is available on creating policies but not on the actual implementation, maintenance and enforcement of a policy. Few seem to be willing to share their experiences with security. This is likely to be due to the fact that it could detract from their image or could highlight weaknesses in their systems that could be exploited by others.

A standard method of researchers in this area is to ignore the documentation of the process, and to rather, give a description of how a policy document should look (Leinfuss 1996; Computer Technology Research Corporation 1998; McMillan 1998; State Of Oregon 1998). 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.

Similarities exist between policy development in information system security and in public policy development in that similar steps are undertaken in the development process. Each has steps similar to: simulation, clarification, initiation, implementation and evaluation (Putt and Springer 1989; Henderson 1996). The similarities end, however with policy documentation. By its very nature, public policy development requires significant amounts of documentation about how policies are conceived. This is usually in the form of proposals for policy and eventually in legislative terms and is required for the policy to be developed and accepted (Jones and Matthes 1983). In information system security, policy documentation tends to be the policy its self, no supporting documentation is available. This may be caused by the writers of security policies following one of the many information system “policy writing” guides available which do not require any documentation except for the policy.

INFORMATION SYSTEM SECURITY EVALUATION

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 1995). 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. Computing has moved to the masses and, as a result, many changes have occurred causing the evolution of this baseline for security.

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). These criteria formed a base standard for security evaluation throughout the European region. 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).

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. The TCSEC and ITSEC are similar, but the ITSEC tends to place more focus on effectiveness (doing the right job) and correctness (doing the job right). This results in a slightly less restrictive, but more complicated evaluation.

In 1993 a new US standard Federal Criteria began development, 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). Its aim is to have an internationally accepted (ISO) standard for the evaluation of information technology that can be used to eliminate the costs of products undergoing multiple evaluations one for each country.

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. 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 organisation with a security policy that is substandard, incorrectly implemented, or even missing. 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. This seems fair for systems that do not have national security implications.

Throughout the development of these security evaluation criteria a common driving force has been responsible: ensuring that the information within the systems is kept secure and available for use. Overbeek (1995) suggests that there were several driving factors for security evaluations that caused the progression of security evaluation criteria from the TCSEC standard towards the Common Criteria standard now being proposed and implemented. These factors include:

- Software producers, rather than national agencies were requiring that their products be classed as secure.
- Development in information technology requires that security criteria frameworks are flexible
- Usage of information technology has changed causing new concerns for security
- Globalisation of products and thus product security evaluation is occurring
- Cost of security evaluation was becoming more of an issue

Whilst this moment towards a global evaluation method of evaluating the security of products is fine, we are still left with the possibility of well-evaluated products being used in

companies with lax security standards and with security policies that may be inadequately defined.

A FOCUS ON EVALUATING POLICY DEVELOPMENT AND OUTCOMES

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 organisation'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 organisations to the current practice in software development, the documentation coming out of the 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 documentation in development is quite evolved and, as a result, the failure of many projects has been avoided through the use of the prior documentation. Similarly, providing the product security evaluation with the required documentation may enable the evaluation to identify possible improvements in the policy development process.

There are many authors, who describe in a normative manner how a security policy should be written. None however, describe the importance of documentation within security policy development. Most 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 organisations 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 organisations 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 organisational 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 organisational 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.

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.

Apart from a lack of documentation, there are several further problems with information security policy development. Warman (1995) states that security policy formation is only being carried out at a low level in organisations. 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. He finds that security issue recognition is gaining importance (and therefore being dealt with at a higher managerial level) within organisations, but that the progress is slow. This is directly opposite to the views of normative writers on the subject (who state that there is high management involvement in policy development), which may either suggest that the theory is incorrect, or that organisations 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 organisations [which does not follow the theory]".

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 organisation. 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 organisation 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 organisation, 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. The newest product evaluation method (CC) is designed to be widely applicable and accepted. Its target is to protect confidentiality, integrity and availability of the system. The common criteria method is designed to be flexible and has clear targets set before a product can be considered secure. It is also a stimulus that enables companies to get products 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 organisation 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.

CONCLUSION

This paper provides a preliminary focus of issues that need to be addressed in the development of security policy in organisations. It proposes some security evaluation practices that may be appropriate for use in the evaluation of the development and implementation of information system security policy.

We have found some identifiable areas where similarities exist in 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 suggest that organisations are not applying this to their policy development.

As a result of these issues, we suggest that a better method of security policy development would be advantageous. We compare this with the manner in which products are developed and the documentation procedures that are used in the development process. It may be possible to redefine the security policy development process to enable self-documentation throughout the process. This will enable the security policy to be evaluated as a whole, using the development documentation to support the evaluation process.

The paper argues that some of the techniques and criteria used in system security evaluation may be appropriate for use in the evaluation of security policy. The paper not only proposes that documenting the development of a security policy is important, but also argues that this documentary evidence can improve the evaluation of a security policy. The manner of documenting the development process however, needs to be investigated.

FUTURE WORK

We are currently undertaking further work in the area to identify an appropriate documentation mechanism for security policy development. In the process of the research a set of evaluation criteria for the evaluation of IS security policy development will be defined and a classification of security policy types will possibly result. We find that many issues are unresolved at present in the area of policy development and evaluation. Several new projects may result as an outcome of these issues.

REFERENCES

Computer Technology Research Corporation (1998). Security Policy : Key to Success. Internet and Intranet: Business and Technology Report. **1:** 1-13.

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.

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." .

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

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

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

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

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

McMillan, R. (1998). Site Security Policy Development, McMillan, Rob.

Nash, M., D. Brewer, et al. (1991). Security Criteria Harmonisation: The Information Technology Security Evaluation Criteria. 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.

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

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

Solsource (1998). Corporate Security Policy, Solsource.

State Of Oregon (1998). Guideline for Developing an Agency Information Systems Security Policy.

US Department of Defence (1995). DOD - Trusted Computer System Evaluation Criteria, US Department of Defence.

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

COPYRIGHT