Evaluating IS Security Policy Development

S.B. Maynard[1] & A.B. Ruighaver[2]

Department of Information Systems

University of Melbourne

Australia

[1]Email: seanbm@unimelb.edu.au

[2]Email: anthonie@unimelb.edu.au

ABSTRACT

Rapidly increasing threats to the security of information systems is forcing organizations to put more effort into improving security policy quality. 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 on the content of the policy, and also on the documentation of why content is there and for what reasons. This will enable a proper evaluation of the quality of the resulting security policy, similar to the state-of-the art evaluation standards used in information technology security evaluation

Keywords :Security Policy, Policy Development

INTRODUCTION

In many organizations, especially in small and medium sized ones, securing the organizations' information is not considered to be a core business objective. Small to medium businesses frequently underrate the risks to their valuable information assets; underestimating how costly it would be if it fell into competitors' hands or was misused.

Surveys conducted over the past 5-10 years have shown organizational interest in security is on the increase and that an upsurge in the implementation of security measures, including the development of organizational security policies, is taking place (James and Coldwell 1993, Ernst and Young 1995, Kearvell-White 1996, Davis 1996, Ernst and Young 1998). What these surveys do not show, however, is whether the quality of the organizations response to the acutely increased threats over this period has been adequate or not.

For an organization to have an adequate response, it needs a properly documented Strategic Information Security Policy. In this research the term Strategic Information Security Policy (SISP) is defined as a set of rules and procedures designed at the strategic level of an organization aimed to protect the information assets of the organization. The quality of this security policy has considerable impact on its capacity to implement adequate measures to prevent, or react to, security attacks as well as its capacity to limit the damage these attacks may cause.

A security policy forces a company to plan for the possibility that their information system may be 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 security policy is enforcing

some protection of the organization's information. Possible problem areas are identified and are acted upon when the policy is implemented.

Our research, in particular, concentrates on how we can improve the quality of the strategic information security policy, which an organization produces. Several issues that need to be addressed are evident:

- How do organizations develop state-of-the-art strategic information security policies?
- Is the development of these policies conducive to their latter evaluation?
- What are the factors organizations use to test whether the policy is a success?

Research on each of these areas tends to be very normative, stating only what should be done, without any obvious evidence of practical application within organizations. Published research on what is actually happening within organizations is rather scarce. 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]'.

There is an extensive body of research on security audits; the evaluation of a particular company's systems to determine if they are secure, sometimes with and other times without reference to the security policy that the company has developed. Such audits focus on the evaluation of whether hardware, software and personnel can be considered secure and whether the policy implementation is still satisfactory. The premise used here is that because the company has a security policy and because we are testing the security of the company's systems, then that security policy by inference is also evaluated. This does not take into account the problems involved with the development and maintenance of the security policy, which in turn may signify that aspects of the policy are not appropriate in some situations. In no research, to the author's knowledge, has the security policy itself been the target of evaluation techniques from either the development or use perspective.

In this paper we attempt to initiate the development of security policy evaluation principles. We first discuss the development of standards for information system security evaluation in general. Then we argue that a similar approach to evaluation should be used for Strategic Information Security Policies. Following this we focus on the policy development process and discuss the need to further improve the re-use of security policies. Finally, we compare policy development with information systems development and emphasize the importance of adequate documentation of the policy development process.

INFORMATION SYSTEM SECURITY EVALUATION

The 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). For several years this was the baseline for security evaluation particularly in 'high risk' government institutions, but also in some commercial situations. However, since the publication of these criteria, significant changes to the computing industry have taken place causing evolution from this baseline.

Since 1995 there have been many attempts to develop a standard form for security evaluation. 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).

These security evaluation standards do not just focus on the evaluation of finished products but also on the development process. 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. 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 organisational 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 organisations, 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.

The question to be asked, therefore, is how one should evaluate the security of an organization. Is it sufficient only evaluating the end product, or should one also evaluate the process used to produce the required level of security. As we believe that the Strategic Information Systems Security policy is one of the major corner stones of an organizations security, the same question should be asked on how to assess the quality of this policy. In our view, the evaluation of the policy itself will have no merit without an evaluation of the policy development process and, if relevant, an evaluation of the policy's maintenance.

SECURITY POLICY DEVELOPMENT

A review of literature reveals several different process models, which organizations can use for the development of custom security policies. Many of them make no distinction between the different kind of security policies for which they may be used and almost all concentrate more on the full life cycle of a security policy and omit any serious discussion on the major issues encountered in the actual policy formulation.

The development process that is probably the most focussed on policy formulation is the one proposed by Bayuk (1996). Essentially the process starts after the identification of the assets to be secured, and goes through a series of prototype documents, and results in the production of a draft policy. After this policy is approved and published, part of the process repeats itself to ensure that the policy is continuously updated. Still most of the model accentuates the need for the actual management of the security policy development process and the actual advice on how the teams responsible for drafting the documents should approach their task is minimal.

Another example of a process of security policy development is presented by Control Data (2000). They use a three-phase process: Policy, Enforcement, and Assurance, which describes the life cycle of the security policy. With this method, the development of the policy, including identifying the threats and risks, is done in the policy stage and enforcement focuses on the action of a security policy. This is where the policy is in use and is constantly monitored and tested by the organization's day-to-day activities. The Assurance phase is where the implementation of the policy and its strategy effectiveness are tested. Additional factors about the success or failure of the policy arise and are fed back to the policy stage. With this particular process some documentation takes place that will allow some indication of why things were done in a particular manner, and may enable an audit trail.

There are a number of other less well-described development processes available in the literature. Each of these policy development processes has many common factors, which we summarised in Table 1.

Table 1
A summary of other process oriented development methods

Author	Woodward (2000)	DTI (1999)	Computer Technology Research Group (1998)	State of Oregon (1998)
Title	*Steps in planning a security policy*	*How to develop a security policy*	*Developing a security policy*	*Guideline for developing an IS security policy*
Steps	1. Study Risk	1. Research policy content	1. Determine what assets need protection	1. Develop a work group
	2. Formulate Policy	2. Draft policy	2. Determine the level of protection for each asset	2. Brainstorm and develop policy points for review
	3. Develop standards about why something should happen and the issues involved	3. Obtain management approval	3. Determine internet usage	3. Once reviewed, develop a draft policy
		4. Issue policy to staff	4. Determine the threats that exist	4. Once finalised, get top management endorsement
	4. Get Co-operation from Management	5. Monitor and maintain	5. Explore how to address the treats identified	5. Brief employees and gain signatures from them
	5. Review		6. Conduct an impact assessment	
			7. Draft a security policy	
			8. Develop an implementation plan	
			9. Add a recovery section in the policy	
			10. User training	
			11. Respond to incidents.	

As can be seen from the table, each of the authors offers similar basic steps for the development of a security policy document. Individual authors also put in specific details dependant on the researcher's audience and purpose. Only the methods proposed by Woodward (2000) and DTI (1999) suggest a monitoring and feedback loop. DTI (1999) does not formally include this as part of the policy method, but as part of developing security for an organization. In each of the methods there is some sort of assessment of what needs to be protected, then the development of policy statements takes place.

In practice, there is not much evidence that any of the above processes are rigorously followed in industry. There is anecdotal evidence that most small to medium sized organizations find these development processes much too expensive and just borrow security policies from other organizations, deleting and adapting policy statements not relevant for their situation.

Even many larger companies do not develop security policies from scratch. They use a method, which uses a set of pre-written authoritative policy statements that are used to produce a workable policy. This 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 an organization needs 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 tailer the policy statements for the organization, producing a tailored security policy.

Pentasafe Security Technologies, a company specialising in security policy development uses this approach and sells a document that has 1000+ precise security policy statements that you can select from to make a policy. Other companies offer similar approaches. A report compiled for the Canadian Government suggests that this approach would be appropriate, with some changes, for adoption within government departments (Canadian Government Report 1996). All major areas of security policy are covered and the scope, according to the report, is similar to current Government security policy. Further, the report suggests that the benefits of this method lie in its ease of use, and comprehensiveness.

The approach adopted by Pentasafe categorises the audience for each policy statement, so that the particular policy statement selected is tailored for the particular audience. Policy statements are further categorised based on the environment risk in which the policy will be implemented. So a high-risk situation has a set of policy statements specifically worded for 'high risk' environments. The approach is complete for a high level set of system security policy statements. However, according to the Canadian Government report, it is not valid for lower level policies. Also, this approach does not address the maintainability or enforcement of the policy.

While re-use of security policy statements can be a valid approach to produce high quality policies, there are inherent problems in this method, depending on how the re-use was conducted. If the development process was purely a 'cut and paste' approach without reference to the risks apparent for a particular organization then there is no guarantee that the policy produced will be effective for the organization. If however, the approach used was to identify the risks facing the organization and to then use the 'cut and paste' method, a more organizational focused policy will be produced. The assumption made here about this approach is that the sources of the policy statements are effective policies, and that the statements themselves are of a high quality. To ensure that the resulting policy is of high quality as well, new development processes need to be worked out; processes that emphasise the major issues in the re-use of security policies. While re-use in software engineering is a mature area of research, we have been unable to find any major references reporting on research in the re-use of security policies.

ENABLING THE EVALUATION OF SECURITY POLICIES

In the previous section we started to expose the gap between theory and general practice in the development of security policies. When we compare this general practice with the current state-of-the-art in information systems development other deficiencies will become evident.

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 generally does not occur.

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. Certainly, the security policy itself is already long-winded enough, without having details on how the document was created, who was consulted in its production or how the policy formulation was achieved. Nor will there be any documentation of political problems that may have occurred during the implementation of the policy, or of how to train people about the policy. With the use of documentation techniques during the development of the policy, however, a security policy could become a principles document again. Other issues not dealing with the principles of security policy would be documented elsewhere along with the justification for the policy.

The most important information that is often missing or just inadequate when we attempt to evaluate a security policy in an organization is the requirements documentation. Without a clear understanding of the requirements, evaluation of the quality of a security policy is almost impossible. An analysis of the risks/threats faced by the organization is only part of the requirements needed for the development of a security policy. The organization's objectives and other political issues that influence the development, implementation and acceptance of the security policy are just as important.

The availability of extensive documentation including the outcomes of an extensive requirements analysis will allow the evaluation of the security policy to reach a greater depth, instead of just superficially evaluating the end product. For instance, rather than concentrating only on whether the policy has been implemented in a particular area, the evaluation can now also consider 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. However, security policies vary greatly depending on the context of the organization and one would expect 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

Information System security evaluation research in many instances focuses on the evaluation of how well information systems are secured in relation to some sort of policy statement or security plan. Little research however, focuses on the manner in which security plans (or policies) are developed, and none, to the authors knowledge, attempt to evaluate the process of generating a security plan, or to evaluate the security plans themselves.

This paper provides a preliminary focus on several issues that need to be addressed in the development of security policy in organizations to enable a proper evaluation of these policies. We have found several identifiable areas where similarities exist with the current system security evaluation processes. These methods of security product evaluation do not merely evaluate the finished product, but attempt to evaluate the complete development process. This not only makes the evaluation process more comprehensive, but also aids in the quality assurance of the product.

In comparing the security policy development process occurring in many organizations to the current practice in information systems development, it becomes evident that the documentation coming out of the policy development is currently negligible. In fact, in real terms, documentation of security policy development is in the 1970's when compared to software development efforts. From the information systems development perspective, the documentation in software 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 security policy evaluation with the required documentation may enable the evaluation to identify possible improvements in the policy development process.

References

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

Canadian Government Report (1996). Information Security Policies Made Easy - Version 4, Baseline Software Inc. USA.

Control Data (1999). Why Security Policies Fail.

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.

DTI (1999). The Business Managers Guide to Information Security, Department of Trade and Industry UK, http://www.dti.gov.uk/cii/docs/bus_man_guide.pdf, Accessed January 2002.

DTI (2002). Information Security Breaches Survey 2002, Department of Trade and Industry UK, http://www.dti.gov.uk/cii/docs/sbsreport_2002.pdf, Accessed September 2002.

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 (1998). 'The Ernst and Young International Information Security Survey 1998'

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.

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.

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.

Woodward, D. (2000). Security Policy Management in the Internet Age. 2000.