An information security meta-policy for emergent organizations

Richard Baskerville and Mikko Siponen

The authors

Richard Baskerville is a Professor of Computing Information Systems, Georgia State University, Atlanta, Georgia, USA.

Mikko Siponen is an Assistant Professor, Department of Information Processing Science, University of Oulu, Oulu, Finland.

Keywords

Security, Information systems, Policy management, Corporate policy

Abstract

There is an increasing movement towards emergent organizations and an adaptation of Web-based information systems (IS). Such trends raise new requirements for security policy development. One such requirement is that information security policy formulation must become federated and emergent. However, existing security policy approaches do not pay much attention to policy formulation at all – much less IS policy formulation for emergent organizations. To improve the situation, an information security meta-policy is put forth. The meta-policy establishes how policies are created, implemented and enforced in order to assure that all policies in the organization have features to ensure swift implementation and timely, ongoing validation.

Electronic access

The research register for this journal is available at
http://www.emeraldinsight.com/researchregisters

The current issue and full text archive of this journal is available at
http://www.emeraldinsight.com/0957-6053.htm

Logistics Information Management
Volume 15 · Number 5/6 · 2002 · pp. 337–346
 · ISSN 0957-6053
DOI 10.1108/09576050210447019

Introduction

There is wide agreement that good information security policy is the foundation of organizations' information security (e.g. Parker, 1998; Perry, 1985; Schweitzer, 1982; Warman, 1992). However, we find very little research into the creation of good security policies. Not surprisingly, varieties of beliefs with respect to security policy exist. Of these different views, two schools of thought can be distinguished:

(1) technical/computer security; and
(2) non-technical/security management.

In the technical discourse, security policy is used as a synonym for overall security architectures of operating systems (Viega and Voas, 2000). More commonly, computer security researchers use the term "policy" for describing access control rules for a computer system (e.g. Sandhu and Samarati, 1994). Sterne (1991) is somewhat between these communities, distinguishing three forms of policies: the security policy objective, the organizational security policy and the automated security policy. The security policy objective is "a statement . . . to protect an identified resource from unauthorized use". The organizational security policy describes how to achieve the specified security policy objectives. The automated security policy refers to the restrictions specifying how a computer system protects computer resources according to an organizational security policy. Abrams and Bailey (1995) differentiate three views concerning policy:

(1) corporate security policy (top management's view);
(2) organizational security policy (users' view); and
(3) technical security policy (designers' view).

Tanenbaum (1992) stresses the separation between policy (what should be protected) and mechanism (how the policy is enforced). As for a view from the school of information security management, Schweitzer (1982, pp. 30-32) takes wisdom from *Webster's Dictionary* defining policy as "a definite course or a method of action". In his account, policies are at top level whereas standards are at middle level. He reserves term procedure for the lowest level directive, establishing how exactly things described in policies are to be done. Wood (1999) espouses that "policies"

Logistics Information Management
Volume 15 · Number 5/6 · 2002 · 337–346

are general management level statements whereas "standards" are more specific and refer to particular technological solutions. For Wood, "guidelines" are similar to "policies", the difference being that "guidelines" are optional while "policies" are mandatory. Dhillon (1997) distinguishes strategy, policy and operating procedures emphasizing that, instead of policies, organizations should form an information security vision and strategy at the top management level.

To avoid confusion in this terminological jungle, a simple three level division of security policies is proposed. In a high-level reference, a security policy is a high-level overall plan embracing the general security goals and acceptable procedures. In a lower level reference, policies are defined information security methods of action that are selected from among alternatives and in light of given conditions that guide and determine present and future information security decisions. The third level is meta-policy (see below).

In spite of the commonly recognized importance of security policies, it is peculiar that current discussion about security policies has been concentrated on specific content issues (e.g. Anderson, 1996; Kwok and Longley, 1997; Parker, 1998; Perry, 1985; Wood, 1995, 1996a, b) and the problem of achieving management commitment with respect to security policies (e.g. Kwok and Longley, 1997; Perry, 1985). Consequently, information security policy formulation is often reported to be an *ad hoc* process (Gaskell, 2000; Sibley, 1993).

Traditionally, the role of general information security standards/guidelines/evaluation criteria in the business of security management, such as BS 7799 (BSI, 1993) or GASSP (1999), have been highlighted (Caplan and Sanders, 1999; Chokhani, 1992; Fitzgerald, 1995; Janczewski, 2000; Solms, 1999; Eloff and Solms, 2000). In the same vein, it is suggested in the information security literature that security polices should be developed with the help of general information security management standards and guidelines (Gaskell, 2000; Janczewski, 2000):

> ... the best method of the ISP [Information Security Policy] development is to concentrate on the baseline approach [i.e. to implement widely used controls] and to implement as much as possible the security standards described [BS 7799, OECD, Orange Book, The NIST Handbook] (Janczewski, 2000, p. 96).

Even though the adaptation of general information security management standards might shorten the time of policy development (Janczewski, 2000), the use of such standards as a basis for security policy development has several shortcomings. First and foremost, general information security management standards and guidelines fail to pay adequate attention to the fact that organizations differ, and therefore their security requirements will differ (Baskerville, 1993). Second, standards do not take into account the social nature of the problems (Dhillon and Backhouse, 2001). Third, generic standards overlook the normal business requirements of organizations with the result that a conflict between the organization's normal business requirements and security requirements proposed by security standards may arise. Fourth, general standards are broadly written necessitating *ad hoc* managerial decision making and judgment (Ferris, 1994). However, general information security management standards do not provide any help concerning these decision-making problems.

It is recognized by a few authors that organizations have unique security needs (Schweitzer, 1982; Wood, 1999) and dynamic business environments (Schweitzer, 1982) – factors which policy development should take into account. However, efforts to address these issues are few and far between. Yet, trends towards emergent organizations (Truex *et al.*, 1999) and Web-based IS (Isakowitz *et al.*, 1998) strengthen the need for proper information security policy planning. Such a vacuum with respect to policy development is not strange considering that security planning generally has not received the intense interest of the information security community (Straub and Welke, 1998). This paper proposes that the introduction of an information security meta-policy is relevant for tackling the aforementioned problems. The aims of information security meta-policy include establishing how information security policies are created, implemented and enforced.

The remainder of the paper is organized as follows. The second section presents examples of high and low-level policies and discusses the related work. The third section outlines policy requirements of emergent organizations. Information security meta-policy is presented in the fourth section. The fifth section provides a discussion

Logistics Information Management
Volume 15 · Number 5/6 · 2002 · 337–346

considering the limits of this study and outlining implications for research and practice. Finally, a concluding section summarizes the key findings of the paper.

Security policy terminology and research

A high-level information security policy expresses security objectives and concerns at the highest level of abstraction, such as a corporate statement about the importance of the information resource, and defines management and employee responsibility to safeguard the resource. An example of such a policy is:

> Departments should ensure that adequate information security management policies are implemented to protect their information asset. A department's information security plan should be formulated for dealing with risks and potential threats to their information asset in a manner commensurate with the department's business priorities, principles and goals. Security functionality should generally strike a balance between ease of use, relative cost, feasibility and availability of resources (Department of Premier and Cabinet – Victoria, 1998).

Lower-level information security policies follow high-level security policy as responses to identified risks reflecting firm objectives, values, and stakeholder responsibilities. Low-level polices are expressed in a lower level of abstraction than high-level policies. As a result there has to be a match between high and low levels of security policies: lower-level policies should be able to revert to high-level ones by increasing the level of abstraction, and vice versa. Lower-level policies mandate organizational processes and represent how the organization must function with respect to security. Such policies assist the firm in identifying areas of vulnerability and the need for control. They may provide specific security countermeasure alternatives, and often carry a statement of sanction for non-compliance. Typically such policies are approved by a steering committee of managers, which may include specialists in information security, design and development and strategic planning. An example of such a policy is:

> You will be required to change your password at least every 90 days. You will not be allowed to change your password again for 15 days after a change. Your account will be disabled after five failed attempts to log on in 24-hours. Your password must be at least eight characters long and have at least one number and one non-numeric character (Cornell University, 2000).

Lower-level policies may address specific countermeasures, for example, by defining virus scan software. Indeed, firewall configurations are sometimes regarded as low-level policy definition (Gaskell, 2000).

An information security meta-policy is a "policy about policies" declaring the organization's plan for creating and maintaining its information security policies. Such a meta-policy defines, for example, who is responsible for making policies, and when such policy making should take place. Meta-policy in the information security realm has remained implicit, and the processes for making policies are typically *ad hoc* (Gaskell, 2000; Sibley, 1993). For example, in the high-level Victoria information security policy above, the policy discusses implementing policy, but does not define exactly who makes these policies, how they are to be made, and when they are to be made.

The importance of security policy is recognized by the authors of different methods for developing and/or managing information systems. Such methods include:

- checklists and standards (e.g. BSI, 1993; GASSP, 1999);
- logical controls added into data flow diagrams (Baskerville, 1993);
- abuse cases based on use cases of unified modeling language (McDermott and Fox, 1999);
- responsibility modeling (Backhouse and Dhillon, 1996; Dhillon, 1997);
- virtual methodology (Hitchings, 1995);
- a methodology based on Checkland's soft system methodology (James, 1996);
- a modified version of Boehm's spiral methodology (Booysen and Eloff, 1995);
- a meta-notation (Siponen and Baskerville, 2001); and
- a security planning model (Straub and Welke, 1998).

However, these approaches – excluding Dhillon (1997) – do not provide any specific support for developing information security policies.

Additionally, several less systematic frameworks for security management have been put forth including Parker (1998) and Perry (1985). These frameworks present different principles for managing security, but

they do not concern themselves with the issue of policy formulation. Moreover, several ready-made policies (often forming different parts of security policies) are suggested including Anderson (1996); Kovacich (1998); Overly (1998); and Wood (1996a, b). These different proposals and examples of security policies provide little help with respect to policy formulation. For example, Fraser (1997) details who might be involved in security policy setting, and what characterizes good policy, but provides little insight into how this policy ought to be formulated.

Only a few information security experts/researchers have paid attention to meta-policy. Wood (1999) has developed a comprehensive approach to security policy formulation that includes specific instructions for formulating high and low-level polices (further developed by Pentasafe Technologies). Wood mainly focuses on content giving his study a policy "checklist" orientation (i.e. desired policies are selected from the checklist of possible and alternative policies).

The 1999 revision of BS 7799, and its cousin, the ISO/IEC 17799, demonstrate increased attention for meta-policy (see Lillywhite, 1999). As standards generally, the original version was essentially a specification for essential countermeasures (low-level security policies). Although the 1999 revision, BS 7799-1, retains these low-level policies to a large degree, there is an increased emphasis on methods for selecting these low-level policies (Pounder, 1999).

The body of advice represented by Wood and BS 7799-1 might each be viewed as a meta-policy. However, of these works, Wood's study appears to be the only approach that is complete enough to be easily adapted as a meta-policy in a large, complex organization.

Emergent organizations require meta-policy

Organizations should be increasing their interest in information security meta-policies due to the increasing rate of technology-driven change in today's commercial, industrial and government organizations (with the Internet as pacemaker). Competitive organizations (and their information resources) must be flexible or even fluid in order to adapt quickly to shifting demands. In order to do this, a business security strategy and a security vision, in terms of Dhillon (1997) including meta-policy, must exist.

Organizations (and their concomitant information systems) that are constantly changing are known as emergent organizations (Truex *et al.*, 1999). Every feature of these emergent organizations is continually in motion, following no predefined pattern. Organizational features that might be thought of as a stable structure, become products of constant social negotiation and consensus building. Consequently, organizational emergence recognizes a theory of social organization in which stable structures cannot be relied upon. Organizational emergence forces security designers to reframe their assumptions about the environment with which information systems must cope. Long system life spans and low maintenance give way to flexible, adaptive (and high maintenance) systems (Truex *et al.*, 1999). Under these goals information security must facilitate rather than inhibit organizational change.

Constant organizational change cannot be easily accommodated by high-level or low-level information security policies. The opportunity to enable and facilitate organizational emergence arises in meta-policies. In order to adapt and yield, security policies should be as changeable as the organizations they protect. However, such adaptation cannot be wholly uncontrolled and haphazard. Hence, emergent organizations must address their needs for flexible, adaptive information security by setting supportive meta-policies. These meta-policies describe exactly how and when information security policies are made (or changed).

Features of emergent organizational security landscape

Fast-paced organizational change denotes a social organization that inhabits a different landscape than might be perceived when an organization is seen as stable and unchanged. For example, emergent organizations are typically highly decentralized in the way the organization attempts to achieve structure. Control over rules, relationships and processes, tends to slip away from a central source of control. From a security perspective, this feature in the landscape

suggests that fixed, centralized security policies are less likely to be as effective as changeable, decentralized security policies.

The security landscape of emergent organizations turns out to be self-management, and consequently raises the ease of use conflict. Security policies must be well motivated (they make sense for different computer users to follow), easy-to-use and well matched to the easy operation of information technologies. For example, policies to which people find it difficult or irrational to adhere are not likely to gain approval or implementation in an emergent organization. However, the decentralized landscape is likely to promote innovation and, given the proper motivation, policies that meet security goals while retaining ease of use are more likely to emerge.

However, because the landscape incorporates so much change in the organization, policy testing becomes a more important feature of this emergent information security meta-policy. Security policies will have to be routinely tested for effectiveness and validity. Such testing will enable the organization to know if its security policies are still providing protection despite possible dramatic organizational changes. Yet, the testing should ensure that the low-level policies match with high-level polices and vice versa. Consequently, a security policy test-and-revise cycle becomes a much more important and frequent security activity. Interestingly, the testing requirement means that implementation must be explicit. Testing a policy means that its expected conditions and outcomes must be very clearly expressed in order to check its operation. This requirement means that the making of security policy must also be a more intensive and careful activity.

The policy-making activity is made even more intensive and careful by the technology demands of emergent organizations. Fast-moving organizational change means fast-changing information requirements. As a result, limited access to information through stringent access control can become a drag on organizational change and thereby threaten organizational survival. This problem is different from the typical ease-of-use issues. This problem is one of limiting organizational emergence because of limited information access. This problem presents conflicting and stringent demands for security policy making, particularly regarding the privacy rights in the face of requirements for absolute accessibility. Compliance with relevant laws both for security and accessibility of private data will not permit the uncontrolled access that emergent organizations seem to demand.

This critical accessibility feature in the emergent security landscape must not be seen as an insurmountable obstacle to flexible and fluid organizational information resources. Rather it highlights the need for security meta-policy that facilitates rapid change and adaptation in access control policies. As the organizational need for information shifts, security policies must be synchronized so as to enable the information access necessary for the organization to function successfully in its new form.

As organizations move toward fast-paced change and become emergent, it is not necessary to constrain this emergence by increased rigidity and centralization in security policies. Rather, it is possible to enable this emergence by increasing the security policy-making activity such that security countermeasures are always in synch with the organization's business requirements. This fast-paced security policy making must be carefully enabled by its clear definition in the organization's security meta-policy.

Security meta-policy imperatives

In order to function effectively in emergent organizations, there are three imperatives that an organizational meta-policy must keep in view. These include suppleness, political simplicity and criterion-orientation.

Meta-policies should enable the organization to be supple in the way it makes and maintains its security policies. When the organization seeks to change in ways that conflict with its existing security policies, the organization meta-policy should facilitate a rapid reaction in the adjustment of security policies. This does not mean that security goals are ignored, rather, it means that organizational security elements are quickly reoriented to allow the organization to achieve its functional needs and its security goals. This supple view on policy makes security policies more responsive to organizational change and has the effect of improving the overall security posture. This posture

Logistics Information Management
Volume 15 · Number 5/6 · 2002 · 337–346

improves because the organizational security policies are always in synchronization with the organization's primary goals and processes for achieving those goals.

Political simplicity can improve meta-policy suppleness. Organizational politics in emergent organizations, owing to the constant change, are complex and difficult to control. The vanguard of organizational change can easily create conflicts with obsolescing policies. The political goal of organizational meta-policy is to maximize policy compliance without totally outlawing non-compliance where situations warrant. This is very soft political territory. What emergent organizations need in terms of security policy non-compliance is for the relevant managers to consider carefully the context and the security policy and make any exceptions to security policy that are both carefully reasoned and explicit. What emergent organizations do not need are harsh, inflexible policies that force change agents into secret and poorly considered non-compliance.

An example of political simplicity can be found in the "soft controls" used successfully in many organizations to control the diffusion of incompatible microcomputer technologies in the early 1980s. Couger (1986) described three approaches to configuration control of desktop computers that he studied in large organizations. The first approach was *laissez-faire*, in which divisions were allowed to adopt any desktop configurations. This approach resulted in widespread incompatibility in desktop technologies. The second approach was hard controls. Centralized decisions were made about allowed desktop configurations and divisions were required, under penalties, to acquire standardized configurations. The results from this approach were strangely similar to *laissez-faire*, because the central standards typically did not match needs in the organizational divisions. The third approach was soft controls. Incentives, such as budget supplements, were put in place to encourage the divisions to acquire their desktop technologies through a centralized organizational agency. Popular configurations were adopted as informal standards that were more heavily supplemented than unusual configurations. This combination of market-driven standards and central incentives resulted in the most standardized desktop configurations in the organizations studied. Deviations from the standards were permitted, but the internal economics of the organization forced deviant decisions to be made with care and understanding. If there was enough deviation, the central standard was changed.

The last imperative is criterion-orientation. In a setting where an organization is emergent, it is important that the policy makers understand and operate with the essential goals of the security policies in view. The meta-policy must explicitly focus the policy makers on the priorities of the organization. For example, a meta-policy might state that the organization must, at all times, keep the organization in compliance with the UK Data Protection Acts. Such a meta-policy focuses policy makers on a criterion that must be met by the changing form of all security policies. However, by not specifying exactly how the criterion is to be met, this allows policy makers to be flexible and adaptive in changing organizational security policies such that the organization can effectively and continuously meet the criterion as the organization emerges.

Meta-policy and policy features

The objective of a meta-policy is to control policy making: how policies are created, implemented and enforced. Some security policy features are considered below.

Policy requirements

There are two essential requirements that must be encompassed by a process of creating information security policies. These are the identification of security subjects and objects, and the classification of security subjects and objects. The meta-policy must ensure that these requirements become primary features of the organization's security policies.

Identification of security subjects and objects. The meta-policy must insure that policies are made that identify security subjects and objects. Security objects are the security relevant assets of the organization. Security subjects are different entities that operate on, or are associated with, the security objects and assets.

The term "security subjects" refers to the different entities that have a relevant security connection to the assets of the organization (security objects). Security subjects may include employees of the organization, business partners and third-parties. The term security objects refers to the assets of the

organization that are particularly relevant to information security. Such assets may range from physical things such as paper to electronic entities such as files. Because organizations differ, they necessarily regard different things as their assets. This difference means that a universal list of assets cannot be provided. We should note, however, that while employees might be regarded as assets of organizations, for security policy purposes, they are classified as subjects.

A classification of security subjects and objects. The meta-policy must insure that policies are made that not only identify security subjects and objects, but also classify these according to access requirements. The resulting security policy must define the framework by which rules might define the various kinds of subjects might access the various kinds of objects. These classifications extend to enable the organization to define the kind of access to objects that the subjects need. Hence, three classifications (subjects, objects and access) are needed.

Information security policies should also elaborate a process by which the organization will determine which security subjects (e.g. employees) need access to security objects, and what type of access (e.g. read, write) the security subjects should have. The process should encompass activities by which certain kinds of access are prohibited and actions that are unnecessary are specified.

Design processes

Organizational information security meta-policy must specify the process by which policies are designed and implemented. These policies must be created such that the proper level of abstractions and expression forms are determined.

Creation of policy and sub-policies hierarchy. The meta-policy will have to encompass activities by which policy requirements will be analyzed and shaped into a hierarchy of high-level polices and low-level/sub-policies (or perhaps further into guidelines and procedures). The policy makers will need to determine what low-level/sub-policies are needed, and what are the target objects and subjects of each particular low-level/sub-policy.

Low-level policies are necessary because differing organizations will have differing complexity in terms of the kinds of subjects and objects. Widely different low-level security policies (e.g. security guidelines for different end-users) will be needed to ensure appropriate security at varying levels of organizations.

Adjusting the levels of abstraction and enforcement needed. The meta-policy will have to prescribe activities by which policy makers can adjust the policies to the best level of abstraction. Consequently, they can set the granularity of the different security policies and concentrate resources on the most important access elements for the particular organization. The meta-policy must also determine the proper expression of the different policies; e.g. formal, semi-formal or natural language.

The meta-policy should also define how the policies are distributed and the implications of the policies. Once the policy is made, organization stakeholders will need to learn about the changes and requirements. Policy makers will need to decide whether internal publication is sufficient, or if training or briefings are required. The meta-policy should also include processes by which policy makers decide how the policies are to be enforced. For example, some policies might be enforced automatically with computer technology (e.g. access control software), politically (e.g. through personnel sanctions) or socially (e.g. using change agents, champions or security awareness).

Each low-level security policy may need a different level of abstraction, a different expression form or a different enforcement mechanism to reflect the target objects and subjects of the policies. Also the design of meta-policy should help policy makers decide what implications may arise with the promulgation of the policies in the organization, their implementation of the policies and their enforcement. It is crucial that different employees of the organization are committed to security policies of the organization and the costs of implementation stays within the budget.

Implementation

The meta-policy must provide processes by which policy makers will determine and specify how the policies are to be implemented. This implementation varies depending on the organization. Emergent organizations are constantly shifting form and culture. This emergence means that implementation processes may have to vary

Logistics Information Management
Volume 15 · Number 5/6 · 2002 · 337–346

according to how dramatic the security policies have changed, and the degree to which the organization must change in response.

Testing
Implementation of policy in emergent organizations is complex and interactive. A policy change is a stimulus for an organizational change, and the exact reaction of the organization will have to be studied. The goals of the policy makers may certainly be effectively achieved as they have designed. However, it is always possible that new policies may be ignored, circumvented or perverted to support goals other than those of the policy-makers.

Consequently testing is necessary. The effects of the policies need to be determined in order for policy makers to know if the goals of the policy have been met, or if the policy needs to be reformulated. In testing, the policies are fully validated. Each policy (high- or low-level) is checked to see whether its implementation meets the requirements and whether the policies are properly enforced.

Discussion, limits of the study, implications for research and practice

The existing approaches for managing/developing secure information systems do not pay much attention to policy development. We propose an information security meta-policy to fill this gap. Meta-policy takes into account the organizational requirements (the phase of requirements capture), and in this way aims to avoid the problem of developmental duality (the conflict between security and functionality (see Baskerville, 1992)). It is believed that the meta-policy is, in principle, easy to integrate into normal IS development and management. The meta-policy features of requirements analysis, design, implementation and testing has a solid foundation on the systems approach underlying many IS development and management approaches.

Limits of the study
The main limit of the study is a lack of empirical evidence concerning the practical usability of the results. However, since the question of policy formulation has not received much interest – and there are no explicit suggestions with respect to meta-policies – a conceptual proposal for meta-policy, as suggested in this study, is needed as a first step.

Implications for research
This meta-policy can be used to evaluate existing and future methods/approaches in the field of security management with respect to security policies. In other words, future work on information security policies should meet the requirements outlined by this meta-policy. For example, the phase of requirements capture suggests that future methods/approaches for managing security in organizations should concentrate more on policy formulation than on ready-made lists of particular actions (what one should or should not do). Future research is needed to evaluate empirically the practical usability of the meta-policy.

Implications for practice
This study aims to overcome certain vital limits of the general information security management standards and checklists. General standards such as BS 7799 fail to satisfy effectively the stages of the meta-policy. These do not pay adequate attention to the fact that organizations are different. Instead of implementing the solutions suggested by general information security standards, practitioners can use this meta-policy as a basis for developing their own information security standards and security policies.

Conclusions

Today's organizations are increasingly federated and emergent. The use of generic information security management standards as a basis for security policy development is inadequate for emergent organizations since standards do not pay enough attention to the fact that different organizations have different security requirements. Yet, alternative approaches for security management, while improving security management considerably, do not address the issue of policy development seriously enough. To tackle with this problem, this paper proposed a meta-policy for dealing with the policy formulation, implementation, enforcement and validation.

References

Abrams, M.D. and Bailey, D. (1995), "Abstraction and refinement of layered security policy", in Abrams, M.D, Jajodia, S. and Podell, H.J. (Eds), *Information Security – An integrated Collection of Essays*, IEEE Computer Society Press, New York, NY.

Anderson, R. (1996), "A security policy model for clinical information systems", 1996 IEEE Symposium on Security and Privacy.

Backhouse, J. and Dhillon, G. (1996), "Structures of responsibilities and security of information systems", *European Journal of Information Systems*, Vol. 5 No. 1, pp. 2-10.

Baskerville, R. (1992), "The developmental duality of information systems security", *Journal of Management Systems*, Vol. 4 No. 1, pp. 1-12.

Baskerville, R. (1993), "Information systems security design methods: implications for information systems development", *ACM Computing Surveys*, Vol. 25 No. 4, December, pp. 375-414.

Booysen, H.A.S. and Eloff, J.H.P. (1995), "A methodology for the development of secure application systems", *Proceedings of the 11th IFIP TC11 International Conference on Information Security, IFIP/SEC'95*.

British Standards Institution (BSI) (1993), *Code of Practice for Information Security Management*, BS 7799, Department of Trade and Industry, DISC PD003, BSI, London.

Caplan, K. and Sanders, J.L. (1999), "Building an international security standard", *IEEE IT Professional*, Vol. 1 No. 2, pp. 29-34.

Chokhani, S. (1992), "Trusted products evaluation", *Communications of the ACM*, Vol. 35 No. 7, pp. 64-76.

Cornell University (2000), *Computer Account Policy*, Cornell University, New York, NY.

Couger, J. (1986), "*Pluribus computum*", *Harvard Business Review*, Vol. 86 No. 5, pp. 87-91.

Department of Premier and Cabinet – Victoria (1998), *Information Security Policy*, Department of Premier and Cabinet – Victoria, 1 September, available at: www.dpc.vic.gov.au/ocmpol/216e.htm (accessed 30 September 1998).

Dhillon, G. (1997), *Managing Information Systems Security*, Macmillan Press, London.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: toward socio-technical perspectives", *Information Systems*, Vol. 11 No. 2.

Eloff, M.M. and Solms, S.H. (2000), "Information security management: a hierarchical framework for various approaches", *Computers and Security*, Vol. 19, pp. 243-56.

Ferris, J.M. (1994), "Using standards as a security policy tool", *ACM Standard View*, Vol. 2 No. 2, pp. 73-7.

Fitzgerald, K.J. (1995), "Information security baselines", *Information Management and Computer Security*, Vol. 3 No. 2, pp. 8-12.

Fraser, B. (Ed.) (1997), *RFC 2196 Site Security Handbook*, Software Engineering Institute, Pittsburgh, PA.

Gaskell, G. (2000), "Simplifying the onerous task of writing security policies", 1st Australian Information Security Management Workshop, Deakin University, Geelang, Victoria.

GASSP (1999), "Generally accepted system security principles – version 2.0", *Information Systems Security*, Vol. 8 No. 3, June.

Hitchings, J. (1995), "Achieving an integrated design: the way forward for information security", *Proceedings of the IFIP TC11 11th International Conference on Information Security, IFIP/SEC'95*.

Isakowitz, B.M. and Vitali, F. (1998), "Web information systems", *Communication of the ACM*, Vol. 41 No. 7, July, pp. 78-80.

James, H.L. (1996), "Managing information systems security: a soft approach", *Proceedings of the Information Systems Conference of New Zealand*.

Janczewski (2000), "Managing security functions using security standards", in: Janczewski, L. (Ed), *Internet and Intranet Security Management: Risks and Solutions*, Idea Group Publishing, Hershey, PA, pp. 81-105.

Kovacich, G.L. (1998), *The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program*, Butterworth-Heinemann, Boston, MA.

Kwok, L. and Longley, D. (1997), "Code of practice: a standard for information security management", *Proceedings of the IFIP TC11 13th International Conference on Information Security, SEC'97*, Copenhagen, 14-16 May.

Lillywhite, T. (1999), "How to protect your information – an introduction to BS7799", *Management Services*, Vol. 43 No. 1, pp. 20-21.

McDermott, J. and Fox, C. (1999), "Using abuse case models for security requirements", *Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC)*.

Overly, M.R. (1998), *E-policy: How to Develop Computer, E-policy, and Internet Guidelines to Protect Your Company and Its Assets*, AMACOM, New York, NY.

Parker, D.B. (1998), *Fighting Computer Crime – A New Framework for Protecting Information*. John Wiley & Sons, New York, NY.

Perry, W.E. (1985), *Management Strategies for Computer Security*, Butterworth-Heinemann, Boston, MA.

Pounder, C. (1999), "The revised version of BS7799 – so what's new?", *Computers and Security*, Vol. 18, pp. 307-11.

Sandhu, R.S. and Samarati, P. (1994), "Access control: principles and practice", *IEEE Communications*, pp. 40-48.

Schweitzer, J.A. (1982), *Managing Information Security: A Program for the Electronic Information Age*, Butterworth-Heinemann, Boston, MA.

Sibley, E.H. (1993), "Experiments in organizational policy representation: results to date", *Proceedings of the International Conference on Systems*, Man and Cybernetics.

Siponen, M.T. and Baskerville, R. (2001), "A new paradigm for adding security into IS development methods", in Eloff, J., Labuschagne, L., von Solms, R. and Dhillon, G. (Eds), *Advances in Information Security Management and Small Systems Security*, Kluwer Academic Publishers, New York, NY.

Solms, R., (1999), "Information security management: why standards are important", *Information Management and Computer Security*, Vol. 7 No. 1, pp. 50-58.

Sterne, D.F. (1991), "On the buzzword 'security policy'". *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 219-30.

Straub, D.W. and Welke, R.J. (1998), "Coping with systems risk: security planning models for management decision making", *MIS Quarterly*, Vol. 22 No. 4, pp. 441-64.

Tanenbaum, A. (1992), *Modern Operating Systems*, Prentice-Hall, Englewood Cliffs, NJ.

Truex, D.P., Baskerville, R. and Klein, H.K. (1999), "Growing systems in an emergent organization", *Communications of The ACM*, Vol. 42 No. 8, pp. 117-23.

Viega, J. and Voas, J. (2000), "The pros and cons of Unix and Windows security policies", *IEEE IT Professional*, Vol. 2 No. 5, pp. 40-45.

Warman, A.R. (1992), "Organizational computer security policy: the reality", *European Journal of Information Systems*, Vol. 1 No. 5, pp. 305-10.

Wood, C.C. (1995), "Writing InfoSec policies", *Computer and Security*, Vol. 14 No. 8, pp. 667-74.

Wood, C.C. (1996a), "A computer emergency response team policy", *Information Management and Computer Security*, Vol. 4 No. 2.

Wood, C.C. (1996b), "A policy for sending secret information over communications networks", *Information Management and Computer Security*, Vol. 4 No. 3.

Wood, C.C. (1999), *Information Security Policies Made Easy*, Baseline Software, San Rafael, CA.

This article has been cited by:

1. Ibrahim H. Al-Mayahi, Sa'ad P. Mansoor. 2014. Information Security Policy Development. *Journal of Advanced Management Science* **2**:1, 135-139. [CrossRef]
2. Kai S. Koong, Mohammad I. Merhi, Jun Sun. 2013. Push and pull effects of homeland information security incentives. *Information Management & Computer Security* **21**:3, 155-176. [Abstract] [Full Text] [PDF]
3. Karen Renaud, Wendy Goucher. 2012. Health service employees and information security policies: an uneasy partnership?. *Information Management & Computer Security* **20**:4, 296-311. [Abstract] [Full Text] [PDF]
4. Kimberley Dunkerley, Gurvirender Tejay. 2012. Theorizing Information Security Success. *International Journal of Electronic Government Research* **6**:3, 31-41. [CrossRef]
5. Ken H. Guo, Yufei Yuan. 2012. WITHDRAWN: The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management* . [CrossRef]
6. Ken H. Guo, Yufei Yuan, Norman P. Archer, Catherine E. Connelly. 2011. Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems* **28**:2, 203-236. [CrossRef]
7. Elspeth McFadzean, Jean-Noël Ezingeard, David Birchall. 2011. Information Assurance and Corporate Strategy: A Delphi Study of Choices, Challenges, and Developments for the Future. *Information Systems Management* **28**:2, 102-129. [CrossRef]
8. Sanjay Goel, InduShobha N. Chengalur-Smith. 2010. Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems* **19**:4, 281-295. [CrossRef]
9. Yogesh K. Dwivedi, Navonil Mustafee. 2010. Profiling research published in the Journal of Enterprise Information Management (JEIM). *Journal of Enterprise Information Management* **23**:1, 8-26. [Abstract] [Full Text] [PDF]
10. Kenneth J. Knapp, R. Franklin Morris, Thomas E. Marshall, Terry Anthony Byrd. 2009. Information security policy: An organizational-level process model. *Computers & Security* **28**:7, 493-508. [CrossRef]
11. Jan Gayness Clark, Nicole Lang Beebe, Karen Williams, Linda Shepherd. 2009. Security and Privacy Governance: Criteria for Systems Design. *Journal of Information Privacy and Security* **5**, 3-30. [CrossRef]
12. John D'Arcy, Anat Hovav, Dennis Galletta. 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research* **20**:1, 79-98. [CrossRef]
13. Qingxiong Ma, Allen C. Johnston, J. Michael Pearson. 2008. Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security* **16**:3, 251-270. [Abstract] [Full Text] [PDF]
14. Elspeth McFadzean, Jean-Noel Ezingeard, David Birchall. 2007. Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review* **31**:5, 622-660. [Abstract] [Full Text] [PDF]
15. Peter R.J. Trim. 2005. Managing computer security issues: preventing and limiting future threats and disasters. *Disaster Prevention and Management: An International Journal* **14**:4, 493-505. [Abstract] [Full Text] [PDF]
16. Maria Karyda, Evangelos Kiountouzis, Spyros Kokolakis. 2005. Information systems security policies: a contextual perspective. *Computers & Security* **24**:3, 246-260. [CrossRef]
17. Ella Kolkowska, Karin Hedström, Fredrik KarlssonAnalyzing Information Security Goals 91-110. [CrossRef]
18. Kimberley Dunkerley, Gurvirender TejayThe Development of a Model for Information Systems Security Success 341-366. [CrossRef]
19. Kimberley Dunkerley, Gurvirender TejayTheorizing Information Security Success 224-235. [CrossRef]
20. Ken H. GuoKnowledge for Managing Information Systems Security 266-287. [CrossRef]