An Information Security Policy Development Life Cycle

T. Tuyikeze and D. Pottas

School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
e-mail: tite@nmmu.ac.za; dalenca@nmmu.ac.za

Abstract

Despite the fact that the formulation and use of information security policies are commonly practiced and that organizations devote significant resources to information security management, it is commonplace that the application of a security policy fails to accomplish its goals. For example, policies may be issued but not reviewed to include new regulatory requirements or business process changes, thereby resulting in neglect of legal responsibilities and policies that are outdated. The main objective of this paper is to provide a roadmap for information security policy development which promotes sustainability. The paper investigates current literature on policy development methods and compares the various approaches. Based on the result of the comparison, an Information Security Policy Development Life Cycle (ISP-DLC) is proposed. The proposed life cycle approach will ensure that organizational security policies are comprehensive, effective and sustainable.

Keywords

Information security policy, policy development life cycle.

1. Introduction

Today, organizations of all shapes and sizes have to enthusiastically embrace information systems and technologies if they wish to survive and better thrive in an increasingly competitive environment. Consequently, it is vital that security controls are introduced to ensure that information embedded within organizational information systems retain its integrity, confidentiality and availability.

In order for an organization to have an appropriate approach to the protection of their information assets, it needs a well planned and effective information security policy. A policy can be defined as (1) ‘‘a course of action, guiding principle, or procedure considered expedient’’ or (2) ‘‘a certificate of insurance’’ (The American Heritage Dictionary, 2000). Using this definition, von Solms (2004) argues that it can be deduced that a policy refers to, firstly, action that needs to be taken or a procedure that needs to be followed and, secondly, a statement or declaration that can be made. Thus, if the procedure is followed correctly, then the ‘certificate of insurance’ should be intact therefore resulting in an organization meeting its goals and objectives (von Solms, 2004).

The implementation of effective security policies becomes critical specifically in the information security management field. The moral is that no matter how strong the presence of technical controls, security always depends on the people within an organization. In an information security programme, people are often referred to as the weakest link (Grobler, T & Von Solms, SH., 2005). Etsebeth (2006) argues that if an information security breach or incident occurs because of the actions of an uninformed or negligent employee, the board of directors and top management may be held personally liable for the conduct of that employee. Therefore, the human factor should not be ignored. For an organization to have adequate security measures in place, it needs documented policies to govern the actions of its employees.

There is growing consensus both within the academic and practitioner communities that information security policies are the basis for the dissemination and enforcement of sound security practices within the organizational context (Doherty & Fulford, 2005). As David (2002) notes: "It is well known, at least among true security professionals, that formal policy is a prerequisite of security".

In this paper, the importance of having effective information security policies and the potential challenges in implementing such policies, are explored. Five approaches or methods for information security policy development are compared. The results of the comparison are incorporated in an information security policy development life cycle (ISP-DLC) approach. The purpose of developing the ISP-DLC is to provide the means to ensure that information security policies address current and changing organizational needs and business goals and that policy compliance is ensured. This will result in information security policies that are truly comprehensive, effective and sustainable.

2. Importance of having an effective Information Security Policy

An information security policy establishes what must be done to protect an organization's information. A well-written policy contains sufficient definition of "what" to do so that the "how" can be identified, measured or evaluated. Having quality policies to address issues of concern can provide greater depth of coverage in relation to improving the overall security of an organization, and can also prove useful from a legal perspective should the policies ever be questioned. An information security policy should specify an organization's complete policy for information protection. It is normally comprised by a high level policy statement together with additional detailed policy documents. The policies should include all the measures necessary for the organization to comply with legal and regulatory requirements.

The importance of security policy documentation lies in the fact that it will come into play should an information security incident takes place that calls the operation into question (Peltier, 2002). For example, there are a number of anecdotes showing that employees who behave inappropriately cannot be dismissed, as no security policy existed stating their behaviour was inappropriate, even though it was damaging to the organization (Leinfuss 1996; Robinson 1997). It then becomes evident that the policy should be informed by the organization's plans to manage its operational risk and comply with legal, statutory, regulatory or contractual requirements, and should support all efforts to achieve these goals.

Furthermore, even if a company is not legally bound to develop and implement an information security policy, such a policy will prove to be beneficial to the company for the following reasons: (i) Information security policies will strive to find a way to best conduct business while simultaneously protecting the identity, authenticity, confidentiality and integrity of the information assets of the company (Mistry, 2002); (ii) Voges (2002) observes that "Internet law is still very confusing, but enterprises with information security policies in place can protect themselves from unnecessary headaches". He goes on to observe that companies which have an effective information security policy that recognizes and complies with internationally acceptable standards will have a distinct advantage over those companies which adopt a "wait-and-see" attitude. Companies which do not have information security policies in place, or do have such a policy, but the policy is not effectively enforced, are earmarked as being prone to fall victim to attacks from hackers, crackers and other threat agents (Voges, 2002). This will ultimately result in loss of customer confidence and shareholder value.

After reviewing why the need for information security policies exists, it should be clear that companies (and specifically the board of directors) may be labelled as reckless, negligent and irresponsible if they allow the company to function without having an effective information security policy in place. Also, it should be evident from the previous discussion that an important reason for having such a policy is to aid directors and top management alike with concrete evidence to present in court that they have fulfilled their responsibility of due care and due diligence. By managing information according to its value, and by protecting the confidentiality, integrity, availability and privacy of their information assets, organizations can not only meet their legal and regulatory requirements but also realize significant business benefits.

Although the implementation of a comprehensive information security policy provides numerous advantages to organizations, the processes of developing, implementing and adopting an effective one that reflects the organization's vision and mission and, at the same time, entrenches the policy in the organization so that it becomes a normal and acceptable part of day-to-day operations are difficult, at best.

3. Challenges in implementing an effective Information Security Policy

Existing literature has emphasized on the foundation of information security policy development. However, it is not clear how well the methods described in literature are implemented (Maynard, S.B & Ruighaver, A.B, 2003). An Ernst and Young (1998) survey found that maintenance and compliance with policies are not given sufficient attention by those companies that do have such policies. It can therefore be deduced that in many organizations security policies end up on the shelf because of ageing which leads to obsolescence.

Because of the difficulties experienced in developing security policies, the elected authors often turn to other organizations' policies, commercially available sources or templates available from public sources, such as the Internet, for answers to their questions (Karin, H & Eloff, J.H.P, 2004). Often, a lack of skills and understanding contribute to the necessity of following such an approach. The resulting document will, however, not give proper direction for information security within the context of the organization that it must protect.

The formulation of an effective security policy can be a very demanding and complicated activity; therefore, the authors will battle with questions such as what should be incorporated into this important document to ensure that organizations meet legal and regulatory requirements while, at the same time, ensuring that best practices for information security management are in place. Notably, the formulation of the policy is only the start of the process. Maintenance and monitoring for compliance are as important if not more important than this initial step and usually present as additional challenges in the process. The policies should furthermore support and augment the business goals of an organization. Therefore any solution which proposes to address the problem of information security policy formulation, adoption and implementation, must address the challenges that have been highlighted in this section.

4. Current security policy development methods

A review of literature reveals a number of approaches or methods that organizations can use to develop custom security policies. These approaches are subsequently compared in a table format (Table 1), which attempts to group the steps proposed by each source into categories which form part of a similar process. For example, the steps categorized into Group 1, typically relate to the risk assessment process which precedes policy formulation. Group 2 deals with the steps required for policy construction for example, drafting the policy. Group 3 focuses on the policy implementation stage while Group 4 concentrates on policy monitoring and maintenance. Group 5 highlights the key roles for management while Group 6 does the same for staff in general. Note that the numbering of the steps proposed by a particular source is retained even if the steps are not displayed sequentially in the Table due to the requirement to categorize steps in a particular group.

The comparison reveals some similarities where the authors agree on the same steps while also showing the gaps where a particular author has not mentioned any step that the others considered important. For example, DTI (1999) does not mention any actions required as part of the risk assessment group while the Computer Technology Research Group (1998) consider risk assessment as the main step to be conducted before attempting any steps for policy construction.

Author	**Control Data (2000)**	**Computer Technology Research Group (1998)**	**DTI (1999)**	**SANS Institute (2007)**	**Woodward (2000)**
Group 1 **Risk Assessment Steps**	1.Identify possible threats and risks	1.Determine what assets need protection			1. Study risk
	2.Determine assets to be protected	2.Determine the level of protection for each asset			
		3.Determine internet usage			
		4.Determine the threats that exist			
		5.Explore how to address the identified threats			
		6.Conduct an impact assessment			
Group 2 **Policy Construction Steps**		7.Draft a security policy	1.Research policy content	1.Write a policy	2.Formulate policy
		9.Add a recovery section in the policy	2.Draft policy		
Group 3 **Policy Implementation Steps**	3.Enforce strategy to protect assets	8.Develop an implementation plan	3.Issue policy to staff	2.Publish the policy	3.Develop standards about policy implementation
		10.User training			
Group 4 **Policy Monitoring and Maintenance Steps**	4.Test the policy to ensure assurance		4.Monitor and maintain	3.Request policy revision	5.Review
Group 5 **Management Buy-in and Approval Steps**			5.Obtain management approval		4.Get Co-operation from management
Group 6 **Staff Support Steps**		11.Respond to incidents			

Table 1: Information Security Policy Development Methods

As can be seen from the preceding table, the authors offer basic steps for the development of a security policy document. In Section 5, the information gleaned from the analysis presented in Table 1 is collated and supplemented to propose a comprehensive information security policy development life cycle approach, as depicted in Figure 1. In order to achieve this goal, the groups that were used to categorize the steps listed in Table 1, are taken to constitute the phases to construct the proposed Information Security Policy Development Life Cycle (ISP-DLC). For example, Group 1 (Risk Assessment) becomes Phase 1 of the ISP-DLC. The same applies to Groups 2 – 4 which become Phases 2 – 4 of the ISP-DLC. Groups 5 and 6 which together cover the role of management and staff in general, are considered to be applicable to each of the phases of the ISP-DLC. Each of the phases requires direction from management and support from staff. For this reason, management buy-in and approval and staff support are depicted as horizontal bars spanning across all four of the phases of the ISP-DLC. The proposed information security policy development life cycle will then serve as a roadmap for organizations to follow to ensure comprehensive, effective and sustainable information security policies. The ISP-DLC is subsequently discussed in more detail.

5. An Information Security Policy Development Life Cycle (ISP-DLC) approach

The proposed ISP-DLC consists of four major phases: Risk Assessment, Policy Construction, Policy Implementation, Policy Monitoring and Maintenance. Each phase can be expanded into steps detailing the activities that occur within each phase as discussed briefly hereafter. It is important to remember that policy development is an iterative and continuous process. Due to changes in technology, the business environment and legal compliance requirements, the policy implementation phase will always be followed by a maintenance phase which incorporates these changes and a monitoring phase which ensures that the directives of the policy are executed operationally (i.e. policy compliance).

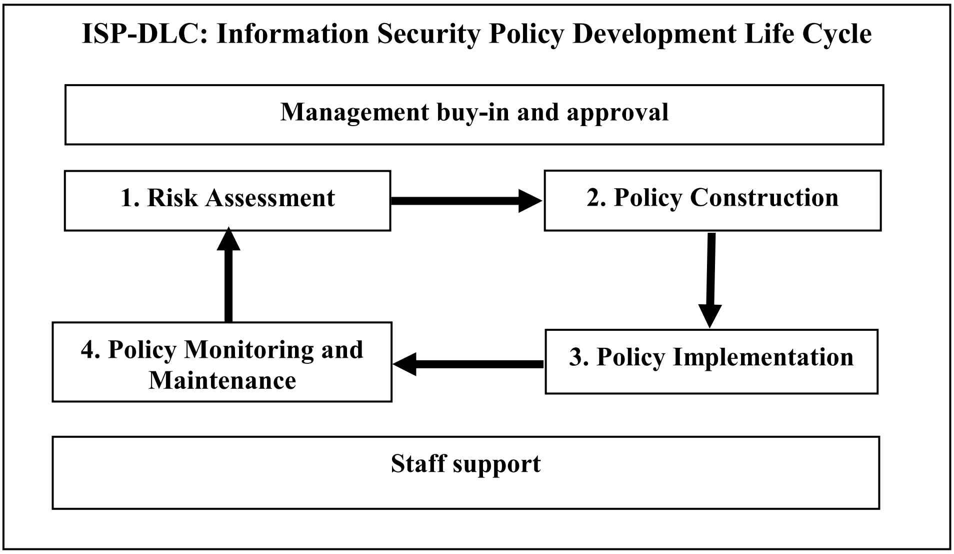
ISP-DLC: Information Security Policy Development Life Cycle
Management buy-in and approval
1. Risk Assessment
2. Policy Construction
3. Policy Implementation
4. Policy Monitoring and Maintenance
Staff support

Figure 1: Information Security Policy Development Life Cycle

Management buy-in and approval is depicted at the top of the ISP-DLC diagram and spans all phases as a crucial component of a successful policy development life cycle. Top management is ultimately responsible for the well-being of an organization. They normally use policies to spell out their management support and direction. Without management supporting security policies, they might be as well be non-existent (Jarmon, D. 2002). These policies need to be communicated to all staff members. The need for staff cooperation is incorporated in the ISP-DLC diagram as a horizontal bar spanning the whole policy development life cycle in a supportive way. Employees need to know what they should and should not be doing, as individuals, in order to maintain the appropriate levels of security. Therefore a communication strategy between managers and staff members is needed throughout the whole policy development life cycle.

The roles of management and staff are further discussed in Sections 5.1 – 5.4 as a sub-component of each of the primary phases by high-lighting issues of relevance to the particular phase being discussed.

5.1. Phase 1: Risk assessment

The risk assessment phase identifies the business assets an organization wants to protect, and identifies potential threats to those assets by asking the following questions:

- What must be protected? (i.e. Assets)
- What must the assets be protected against? (i.e. Threats and vulnerabilities)
- How much is the organization willing to spend to have adequate protection?
- What is the cost versus the benefit for the business?

The phase consists of four sub-steps: Identify the assets, Identify vulnerabilities and threats, Summarize risk assessment results, Evaluate possible measures and controls. These sub-steps must be executed in sequence and the result will be used to decide what to incorporate in the security policies in order to ensure that the identified risks are mitigated.

5.1.1. Management buy-in and staff support (Phase 1)

Based on the result of the risk assessment, management must evaluate the costs and benefits of implementing the recommended controls to reduce risk to an acceptable level. If the envisaged expense is within budget, the next phase of policy construction can commence. If not, the risk mitigation strategies will need to be revised to be within budget or the budget must be increased. At this stage of the policy development life cycle, the involvement of management is a primary requirement, whereas staff in general will only be involved from a risk assessment point of view.

5.2. Phase 2: Policy construction

The security policy is developed during this phase based on the findings and recommendations to reduce the risks posed by threats and vulnerabilities as agreed on in the risk assessment phase. This phase will also consider business strategies and objectives and legal requirements during the construction of the policies. The phase is comprised by the following sub-steps: Draft a one-page policy statement and high level outline of security requirements, Review and approve high level policy statement, Draft detailed policy documents, Review and approve detailed policy statements, Publish approved security policies.

The process of writing the information security policies involves selecting appropriate control objectives that need to be achieved. A control objective is defined as a "statement of the desired result or purpose to be achieved by implementing control procedures in a particular process" (Cobit 4.1, IT Governance Institute). A control objective can also be seen as an information security best practice which is implemented through using appropriate security controls (ISO 27002, 2005). A one page policy statement and high level outline of security requirements to meet the requirements of the selected control objectives will be drafted. This draft provides a starting point to create an ideal information security policy that reflects the top level concerns of the organization. The draft will be submitted to the executive and senior management for review and approval of the high level policy statement. If approved, a draft of a detailed policy document based on the high level policy statement is submitted again to management for approval; and if approved, the security policy is ready to be published.

5.2.1. Management buy-in and staff support (Phase 2)

Except for the integral role of management to review and approve the policy drafts and final security policy documents, their express commitment to and support of the policies are required with a further concerted effort to ensure proper communication of policies to staff. A communication plan that enables audience feedback must be initiated during the policy construction phase to prepare the organization for the upcoming changes and to enable individuals to influence the formation of the new policy. Involvement is critical in moving users through the stages of commitment from preparation through acceptance and ultimately to the commitment stage.

In addition, a new or updated security policy will inevitably change something about the way someone is working, and such changes, no matter how small, require attention. The impact of the change must be assessed to make sure it can be successfully implemented. An understanding of the current environment is therefore vital. For example, these questions should be asked during the policy construction phase to assess the staff's ability to successfully support a new security policy:

- Who is impacted?
- Is the culture conscious of the importance of security?
- How does the culture require that components of a new policy and key implementation issues be introduced?
- What is expected to happen when the new policy is implemented?

The afore-mentioned aspects must then be addressed during the policy implementation phase to ensure staff acceptance and support for the new policies.

5.3. Phase 3: Policy implementation

After completing policy construction, it is time to implement the new security policy document. A detailed implementation plan is now required to translate the design into reality. This phase covers the following sub-steps: Define security and control requirements through detailed procedures and guidelines, Allocate information security responsibilities, Test security and control requirements, Implement security and control requirements, Implementing ongoing security policy training and awareness.

5.3.1. Management buy-in and Staff support (Phase 3)

Communication from senior members of the organization will increase the likelihood of security policy acceptance by the organization as a whole and help to promote individuals through the stages of commitment. The endorsed final copy of the security policy must be made easily available to all employees. It must be communicated to all users formally and users are to acknowledge that the policy is read and understood by signing and agreeing to comply with it. The next requirement will be to develop security awareness and training programs regarding the new policy. These programs are very critical steps of the policy implementation phase as their main role will be to change the attitudes of employees by encouraging them to play an active role in policy implementation.

5.4. Phase 4: Policy monitoring and maintenance

This phase is comprised by two main activities, viz. monitoring and maintenance.

Policy monitoring

After the information security policy has been implemented, organizations should include the appropriate monitoring mechanisms to define the daily activities throughout the organization that ensure the security policy is enforced across the organization. The following sub-steps should be executed: Produce measurable results reflecting users' behaviours, Perform system audits and reviews, Perform intrusion detection and penetration testing, Perform user activity audit trail analysis, Audit policy compliance. The main goal of policy monitoring is to ensure that staff members comply with new policy requirements. In this way, the proposed ISP-DLC shows that compliance with policy requirements is necessary to ensure sustainability of security policies. Policies that are only constructed and never applied and adhered to, are of no use to the organization.

Policy maintenance

This activity incorporates the following sub-steps: Review reports of security incidents, Review security and technology infrastructure, Review business strategies, Review trends and unexpected events, Review legal requirements, Compile request for policy changes, Repeat policy development life cycle.

It is important to review the security infrastructure of an organization continuously to identify new threats. This could be due to changes in technology used elsewhere in the organization. It is further possible that new laws are introduced which would need to be incorporated in organizational security policies. The bottom line is that changes of varied nature, could lead to information security policies becoming outdated. These changes must be incorporated in the policies through the maintenance phase. The maintenance phase requires a re-execution of Phases 1 – 3 in the life cycle in order to ensure that changes to policies are not applied in an ad hoc way. Of course, there are a lot of unknowns and during this phase organizations will likely identify a new threat that wasn't considered, a new technology that is needed, or a business capability that was forgotten and has to be catered for in the organizational policies.

5.4.1. Management buy-in and Staff support (Phase 4)

In this step, management must ensure that appropriate procedures and systems are in place to determine whether personnel understand the implemented policies and procedures and that the policies and procedures are being followed. Furthermore, management needs to ensure that there are appropriate consequences for non-compliance with the security policy requirements. Penalties need to be consistently enforced and communicated to all staff members.

6. Conclusion

Security policy development goes beyond simple policy writing and implementation. Unless organizations explicitly recognize the various steps required in the development of a security policy, they run the risk of developing policies that are poorly thought out, incomplete, redundant, not fully supported by users, superfluous or irrelevant. A security policy has an entire life cycle that it must pass through during its useful lifetime. The objective of this paper was to propose an information security policy development life cycle which will ensure both comprehensive and sustainable information security policies.

Organizations cannot develop comprehensive security policies in one hit; but a well-planned, continuous process must be followed during the security policy development life cycle. It is conceivable that if a security policy has gone through a life cycle more than once, the policy will be more mature both in the sense of supporting the security principles of the organization and it being operationally entrenched in the company through the existence of proper procedures that guide its implementation. The creation of information security policies is not a once-off event but requires continued commitment to ensure that the policies add value. This can be achieved through the proposed life cycle approach. Using the comprehensive security policy life cycle as described here will provide a framework to help organizations ensure that the necessary steps for security policy development are performed consistently over the life of the policy and that the policies are complied with. In this way the policy itself is not the only artefact of the development process, but includes its sustainability and the assurance that the policies are complied with.

7. References

Bindview, 2005. Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs. Available on the internet: www.bindview.com. Sited on 15 September 2005.

Chaula, J.A , Yngström, L & Kowalski, S., 2004. Security Metrics and Evaluation of Information Security Policy, http://icsa.cs.up.ac.za/issa/2004/Proceedings/Research/048.pdf (Accessed 02 February 2008).

Control Data. (1999). Why Security Policies Fail, http://www.securityfocus.com/data/library/Why_Security_Policies_Fail.pdf, (Accessed 12 February 2008).

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

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

DTI. (1999). The Business Managers Guide to Information Security. Department of Trade and Industry, UK. http://www.dti.gov.uk/cii/datasecurity/businessmanagersguide/index.shtml, (Accessed 23 March 2009).

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

Etsebeth, V., 2006. Information Security Policies – The legal risk of uniformed personnel. Information Security Management and Regulatory Compliance in the South African Health Sector. Proceedings of the 6th Annual Information Security South Africa Conference, 29-01 July 2005, Sandton, South Africa.

Grobler, T & Von Solms, SH., 2004. Assessing the policy dimension. Information Security South Africa, icsa.cs.up.ac.za/issa/2004/Proceedings/Full/051.pdf, (Accessed 02 February 2008).

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

Hoepfl, M.C. (1997). Choosing qualitative research: A primer for technology education researchers, Journal of Technology Education, 9(1), 47-63.

ISO/IEC 27002 (2005), Information Technology: Security Techniques – Code of Practice for Information Security Management (Edition 2): SANS.

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

Herold, R., 2004. The Practical Guide to Assuring Compliance, http://www.realtimepublishers.com, (Accessed 08 August 2009).

eHealth Initiatives, 2006. Improving the quality of healthcare through Health Information Exchange. eHealth Initiative' s Third Annual Survey of Health Information Exchange Activities at the State, Regional and local levels.

Krygier, A. (1993). TQM A world view. Journal of Management Development, 12, 36-39.

Janczewski, L. Keng, B. 1998. Privacy protection in hyper-media health information systems from law point of view. In Proceedings of Joint IFIP TC 6 and TC 11 Working Conference on Information Security small systems security & Information Security management. Vienna-Budapest , 2 september 1998.

Joint Information Systems Committee (JISC), Developing an Information Security Policy., http://www.jisc.ac.uk/pub01/security_policy.html, (Accessed 24 march 2009).

Karyda, M & Kokolakis, S & Kiountouzis E, 2003. Content, context, process analysis of IS security policy formation. In: Gritzalis D, et al, editors. Security and privacy in the age of uncertainty, Proceedings of the 18th IFIP international conference on information security. Kluwer Academic Publishers.

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

LEE, A.S. (1999). Researching MIS. In Currie, W.L. & Galliers, R., eds. Rethinking management information systems. Oxford: Oxford University Press. p.7- 27.).

Masters, C., Carlson, D.S., & Pfadt, E. (2006, October). Winging It Through Research: An Innovative Approach to a Basic Understanding of Research Methodology. Journal of Emergency Nursing. Erie, PA.: Emergency Nurses Association.

Maynard, S.B & Ruighaver, A.B. 2003. Development and Evaluation of Information System Security Policies Information Systems: The Challenges of Theory and Practice, Hunter, M. G. and Dhanda, K. K. (eds) Information Institute, Las Vegas, USA, pages 366 – 393.

Jasmine et al., 1999. Trends in quality management research: 1990 – 1996, http://www.entrepreneur.com/tradejournals/article/78630789.html, (Accessed 17 September 2008).

Mistry, 2000. “Developing security policies for protecting corporate assets”, http://www.sans.org, (Accessed 24 July 2005).

National Research Council (NRC), 1997. Committee on Maintaining Privacy and Security in Healthcare Applications of the National Information Infrastructure. For the Record: Protecting Electronic Health Information. National Academy Press. Washington DC.1997, http://books.nap.edu/catalog/5595.html, (Accessed 20 April 2008).

Peltier, 2002. Information security Policies, Procedures, and Standards.

The American Heritage Dictionary. 4th ed. Houghton Mifflin Publishing Company; 2000.

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

SANS Institute 2007. A Short Primer for developing security policies, http://www.sans.org/resources/policies/Policy_Primer.pdf?portal=7f704fb9ef6686500c5876a5a1fd9ae6, (Accessed 10 June 2007).

Spyros, K., Dimitris, G & Sokratis, K., 1998. Generic security policies for healthcare information systems. Health Informatics Journal 1998; 4; 184.

SSE-CMM Project, Systems Security Engineering Capability Maturity Model SSE-CMM Model Description Document, Version 3.0, http://www.sse-cmm.org/docs/ssecmmv3final.pdf, (Accessed 30 June 2008).

Voges, 2002. IT needs security partnership with HR, http://www.computingsa.co.za, (Accessed 20 February 2007).

Woodward, D. (2000). Security Policy Management in the Internet Age, http://www.itsecurity.com/papers/wickpol.htm, (Accessed 10 June 2008).