Information Security Policy

Joel Weise’s and Charles Martin’s article, “Developing a Security Policy” (2001), defines a security policy as a formal document, which specifies rules and regulations that an organisation’s employees are required to adhere to when accessing technology, systems and other information assets acquired by the organisation. The purpose of a security policy is to inform stakeholders of the organisation’s requirements for ensuring the protection of assets, such as; people, data and technology. Another aim is to provide a general yardstick to acquire, configure and audit systems and networks to establish if they are compliant with the policy, in turn this allows for the deployment of system and network parameters to be applied. A security policy should be; feasible, comprehensible, consistent, and realistic and provide reasonable protection to the security objectives outlined by senior management.

Smith and Newton (2000) argue that there are three types of security polices, they are; program policies, system specific policies, and issue specific policies. Program policies in nature are rarely updated and are what management uses to create a security program. System specific policies are regulations in place that are applied to protect a specific information system. These types of policies are regularly updated as system configuration changes which can create new vulnerabilities to address. Issue specific policies address current issues that are affecting the organisation, for example; particular viruses encountered through spam via email. These polices are usually created and circulated when an incident occurs, an almost how to avoid or respond to an incident.
Security Policy Development

Weise & Martin outline a step-by-step guideline on how to create a security policy, addressing the key issues that need to be mentioned. The following are the main tasks they identified:

1. Stakeholders involvement and responsibilities are defined
2. Business objectives are made aware
3. Security principles are developed based on management's security objectives
4. Organisation assets such as data is identified and classified
5. Track data across the organisation using a data flow analysis
6. Identify risks associated with the organisation
7. Security services are identified
8. A generic policy template is developed
9. Security policies are then defined

In contrast, Smith and Newton (2000) propose a three-tier hierarchy that supports the development of security policies and requirements. The top layer represents an organisation's security policies; these are often stated in policy documents such as organisational regulations and directives (they are very similar to Weise & Martin's security principles), they also aid directly onto the program policies, as defined earlier. An example of a level 1 policy requirement would be to prevent unauthorized access to data. Level 2 policy requirements address implementing a specific security component to evaluate Level 1 policies and prevent their occurrence by implementing access controls. The end product of level 2 is the system specific policy (defined earlier). Level 3 identifies the functional and assurance requirements in a system. The hierarchy can be seen in the following figure:
Generally in order to be successful a policy should be developed to meet the CIA model, which incorporates confidentiality, integrity and availability. Confidentiality is the primary focus of security its purpose is to ensure that information is protected and not released to unauthorised persons through any means. Typical objectives of attaining confidentiality is as follows:

- To manage unauthorized access to classified data based on clearance.
- To manage unauthorized access to classified data based on need-to-know basis.
- To manage unauthorized access to unclassified sensitive data.

Integrity in security polices aims to protect against unauthorized alteration or destruction of information and to ensure the correctness and completeness of data. It also directly relates to the reliability of an operating system, that is, is it stable enough to keep out hackers. Some general objectives of integrity are as follows:

- To manage unauthorized modification to system hardware and software.
- To detect unauthorized modification to system hardware and software.
- Prevent unauthorized modification (create, delete, change) of data.
- Detect unauthorized modification of data. (Selectively)

Availability aims to allow for the timely and reliable access to data and information services for authorized users. An example of an objective of availability is to prevent denial of service based on resource exhaustion.
Conclusion

Since the publication of this article industry best practice is no longer an option in regards to security policies, it’s mandatory. The introduction of the Sarbanes Oxley Act 2002 has impacted how organisations, those in particular listed on the US Stock Exchange, financially report. Section 404 of the Act addresses internal controls, which particularly focuses on security measures taken to protect crucial business information. This means that security policies and procedures that organisations implement are not only subject to internal auditing but also external auditing (Colley, Doyle, Logan, Stettinius, 2005). Another section of this Act also requires stakeholders to be required to sign off on the policies created to protect information. This is to display that they have read and agreed to the regulations that the document outlines. Thus should be required to ensure that staff members are held liable for any breach of the contract, this is another aspect Weise & Martin fail to mention in the article. They also don’t address how organisations culture is affected by the implementation of a security policy. Helms argues that comprehensive security policies can create problems of their own, they include; user paranoia, duplication of effort and repressive work atmosphere (Helms et al. 2000: 127, 118). Another criticism of the article is that it clearly omits the concept that no matter how complex and thorough an organisation’s policies and procedures are, there is always some form of threat. Security policies are not the silver bullet in preventing the vulnerability of an organisation. The best that can be done to prevent such an occurrence is to distinguish the appropriate combination of process technology, people resources and unite them to obtain a security framework that can identify risk and withstand it.
Resources


M. Helms et al. (2000) ‘Shielding your company against information compromise’, *IM&S* 8(3).

Hulme, G.V. (2000). *It's Time To Clamp Down.* Information Week Online.
Retrieved, 12th October, 2005 from the World Wide Web:
http://www.informationweek.com/794/security.htm

Retrieved, 12th October, 2005 from the World Wide Web:

Retrieved, 12th October, 2005 from the World Wide Web: