We are currently living in an age of information technology. An age where thanks to the advent of the Internet, geographical and spatial boundaries no longer provide a form of restriction on our findings or requirements. An age where by information is passed freely amongst networks almost with no regard to security or any measures which may be in place. This open forum from which users are able to access information at any given time has proven a clear indication for the importance of a security policy for any organization in protecting their information assets.

A security policy is a plan of action for tackling security issues, or a set of regulations for maintaining a certain level of security. It can span anything from the practices for securing a single computer, to building/premises security, to securing the existence of an entire nation-state.” It is "A formal statement of the rules through which people are given access to an organization's technology, system and information assets... (it) defines what business and security goals and objectives management desires... " (Weise 2001) A security policy to put it simply is a set of rules which govern or encompass the organizations goals and objectives for the use of any respective information. This document is an integral part of any organization as it can assist management if a security breach or threat is violated.

The article discusses the varying degrees involved in the development of a Security Policy. Weise outlines the facets of a Security Policy whilst also calling upon issues pertaining to the various use of communication channels and information flows within an organization. After providing the user an in depth analysis of a Security Policy, he also outlines means by which one can be developed and implemented. The article however fails to depict the broad reasoning for the importance of a security policy and touches only briefly on maintaining aspects of information security within an organization.

As outlined by Weise, aspects of a Security Policy include the following;

Developing A Security Policy

Policy Flexibility
A Security Policy must be flexible in order to adapt to any changes both internal and external to the organization. It must also clearly outline the processes involved in updating the Policy.

Security Policy Communication
A security Policy once finalized must then be disseminated to all appropriate levels of both internal and external staff and stakeholders. If a policy requires notification to the public adequate levels of notification must be undertaken to ensure so.

Policy Management
Management and regular maintenance of the policy must be undertaken to ensure integrity and timeliness of the policy. Weise recommends a specific business unit, such as the Data Security Department, to be given custodianship of the Policy and all updates.

Relationship to Standards and Procedures
The policy should be defined and bound to a set of standards, guidelines and procedures which are in cohesion with the standards and procedures of the organization itself. These set of standards, guidelines and procedures should be utilized as a measure to ensure all operations are consistent with the Security Policy.

Implementation in IT Systems
Once the Security Policy has been established, appropriate parts of the policy must then be implemented. For example, if the policy calls upon biometric data to be utilized for the log in to a set system then adequate hardware and software must be implemented accordingly.

Security Stance
Policies developed should be based upon a formal security stance which is determined by management.

Security Policy Structure
As identified by Weise, the overall structure for a security policy should be as follows:
- A statement of the issue that policy addresses
- A statement about your position on the policy
- How the policy applies in the environment
Developing A Security Policy

- The roles and responsibilities of those affected by your policy
- What levels of compliance to the policy is necessary
- What actions, activities and processes are allowed and which are not
- What are the consequences of Non – Compliance

Weise then further discusses the Roles and Responsibilities of parties within an organization as well as referring to the intended audience of the Policy. Weise then outlines the means of developing a security policy through the use of a development plan.

This article whilst providing a good framework from which to gain an understanding of a Security Policy did not adequately discuss issues such as communication or information flows. There are varying levels of communication within an organization such as the management Level, Ad Hoc Communications, Informal communications, etc.

The Management Level of communications is a ‘formal method of making available to management the accurate and timely information necessary to facilitate the decision making process and enable the organizations planning, control and operational functions to be carried out effectively’ (Stoner, quoted in Brown & Starkey 1994: 810) Whilst the Ad hoc communication methods are the operational communications that do not take place within the context of the formally specified channels. (Brown & Starkey 1994: 810) Informal communications are those ‘grapevine communication which may be loosely work-related but does not involve required operational information’ (ibid). Weise fails to outline the most suitable means by which the Security Policy should be disseminated. Given the importance to the organization, the Security Policy should be disseminated at all layers if possible, this will help to ensure adequate penetration to staff within an organization as well as all external stake holders of the respective security goals and objectives.

Weise also failed to outline the position of the Security document given today’s climate – whilst touching on the importance of a security policy, there is no clear reasoning to show why it must be an integral part of any organization.

\[2\] We are living in an emerging

---

\[2\] Mapping Entry Vocabulary to Unfamiliar Metadata Vocabularies, Buckland M, University of California, Berkeley, 1999
Developing A Security Policy

network environment bringing access to an increasing population of heterogeneous repositories. With this almost seemingly uncontrollable access to information, it brings to light issues of information security.

An important part of any organization is to ensure all data and information held is secure from any threats or possible breaches which might cause the information to lose aspects of confidentiality, integrity, or availability. This forms a risk for an organization, a risk is generally defined as "The possibility of loss" and as it applies to information technology, "the possibility for loss of availability, integrity, or confidentiality due to a specific threat".

A threat is a possible attack on targets, and can encompass any of the following:

- Denial of Services
- Sabotage
- Forces of Nature
- Sniffing
- Eavesdropping
- Theft
- Espionage
- Data/Message Tampering
- Masquerading
- Fraud
- Piracy
- Copyright Infringement

Within any given subset there exists an innumerable amount of malicious codes and viruses which can be applied to any information system. The information of an organization is one of the most important assets to the business itself, and a meticulous Risk Management plan must be in place to protect it from any possible threat or breach which may occur. A Security Policy forms one important aspect of this Risk Management plan, as it provides the organization a formal statement to outline their organizational goals and stances relating to the security and safe guarding of information at hand and also provide a means of audit for those who breach the policy. Weise fails to identify or provide an adequate framework from which the security policy is required,

---

3 Intelligence-Based Threat Assessments for Information Networks and Infrastructures, Accessed 17th October 2005 retrieved from (http://www.aracnet.com/~kea/Papers/threat_white_paper.shtml) 1999
and as such one fails to gauge the importance of such a document. Whilst there exists alternate security measures to combat possible threats or security breaches, a Security Policy must complement these and thus must form a central part of any organization.

References


http://www.dlib.org/dlib/january99/buckland/01buckland.html
