ISSN 2047-3338

Information Security Policy Trend as a Foundation to Protecting Information Resources

Abila James[1], Mutua Stephen[2], Wabwoba Franklin[3] and Anselmo Peters[4]
[2,3,4]Department of Computer Science, Masinde Muliro University of Science and Technology
[1]Asumbi Teachers College

***Abstract*– Although many institutions have implemented technical solutions to protect information resources from adverse events, internal security breaches continue to occur. An approach that emphasizes on information security policy within the institutions is therefore required to make security part of employees' daily work routines. In order to develop a successful information security culture within an organization, it is worth understanding both technical and non-technical aspects of information security. The purpose of this paper is to outline the strategies and management processes behind implementing a successful Security Policy. Additionally, the paper gives recommendations for the creation of a Security Awareness Program, whose main objective is to provide staff members with a better, if not much improved understanding of the issues stated in a security policy.**

***Index Terms*– Education Institutions, Ethics, Information, Security and Policy**

I. INTRODUCTION

INFORMATION security has come to play an extremely vital role in today's fast moving, but invariably technically fragile business environment [1]. Consequently, secured communications are needed in order for both organizations and staff to benefit from the advancements that the Internet is empowering us with. The importance of this fact needs to be clearly highlighted so that adequate measures will be implemented, not only enhancing the organizations daily business procedures and transactions, but also to ensure that the much needed security measures are implemented with an acceptable level of security competency. It is sad to see that the possibility of having your organizations data exposed to a malicious attacker is constantly increasing nowadays due to the high number of "security illiterate" staff also having access to sensitive, and sometimes even secret business information [2]. Imagine the security implications of someone in charge of sensitive company data, browsing the Internet insecurely through the organizations network, receiving suspicious e-mails containing various destructive attachments; the significant threats posed by the constant use of any Instant Messaging (IM) or chat applications among others.

Analyzing human behavior in order to manage security risks is an approach that can directly be applied and will be followed in the next one or two decades. In the long run, information security needs a fundamental change. As societies, businesses and information systems have transformed from isolated entities to hierarchical structures to decentralized systems, information security strategies eventually need to make this last step as well. Gathering more and more information will help decision makers to obtain a clearer picture [3]. With more knowledge, they become able to better regulate the system. However, as with political and economic systems, security managers cannot gather an infinite amount of information, which would be necessary to regulate highly decentralized systems.

The rest of this document is arranged as follows: Section II discusses security policy and its various dimensions; Section III outlines the role of security awareness program towards implementing the security policy while section IV highlights ethics as a fundamental component towards ensuring information security. Section V describes the role of management committee in security policy development and implementation; and finally section VI presents the conclusion.

II. SECURITY POLICY

The security policy is a plan, outlining what the company's critical assets are, and how they must (and can) be protected [4]. Its main purpose is to provide staff with a brief overview of the "acceptable use" of any of the Information assets, as well as to explain what is deemed as allowable and what is not, thus engaging them in securing the organizational critical systems. The document acts as a "must read" source of information for everyone using in any way systems and resources defined as potential targets [5].

A good and well developed security policy should address some of the following elements: how sensitive information must be handled, how to properly maintain username(s) and password(s), and any other accounting data, how to respond to a potential security incident, intrusion attempt, etc., how to use workstations and Internet connectivity in a secure manner and how to properly use the corporate e-mail system.

The main reasons behind the creation of a security policy is to set a company's information security foundations, to explain to staff how they are responsible for the protection of the information resources, and highlight the importance of having secured communications while doing business online [1].

A. Why Security Policy

A good security policy provides the foundations for the successful implementation of security related projects in the future; this is without a doubt the first measure that must be taken to reduce the risk of unacceptable use of any of the company's information resources. The first step towards enhancing a company's security is the introduction of a precise yet enforceable security policy, informing staff on the various aspects of their responsibilities, general use of organizational resources and explaining how sensitive information must be handled. The policy should also describe in detail the meaning of acceptable use, as well as listing prohibited activities [6].

The development (and the proper implementation) of a security policy is highly beneficial as it will not only turn all of staff into participants in the organizational effort to secure its communications but also help reduce the risk of a potential security breach through "human-factor" mistakes. These are usually issues such as revealing information to unknown (or unauthorized sources), the insecure or improper use of the Internet and many other dangerous activities. Additionally the building process of a security policy will also help define a company's critical assets, the ways they must be protected and will also serve as a centralized document, as far as protecting Information Assets is concerned.

B. The Human Factor in Information Security

Even though many educational institutions have not realized it yet, the human factor has an immense impact on information security. In contrast to the general assumption, insiders carry out a large share of security breaches. Even if the attacker is an outsider, social engineering, the art of manipulating people, is becoming a more and more common way of attacking information systems. Social engineering can hardly be prevented by means of technical or organizational countermeasures. Nevertheless, sensitizing and educating staff and students have been a low priority for many security managers for years [7].

C. Policies and Information Security

Information systems security policies primarily address threats. In the absence of threats, policies would be unnecessary—one could do as one chooses with information. Unfortunately, threats do exist and information systems security policies are necessary to provide a framework for selecting and implementing countermeasures against them. An enforceable written policy helps ensure that everyone within the organization coherently behaves in an acceptable manner with respect to information security [5].

A well-designed information security policy defines the objectives of the information system of an organization and outlines a strategy to achieve these stated objectives. Conversely, an information system without security policies is likely to be a disjoint collection of countermeasures that address a variety of threats. Information Systems security policies can often be used to help integrate the many different aspects of an enterprise to achieve business objectives [1].

Policies, standards, guidelines, and training materials that are obsolete and not enforced are particularly dangerous to an organization because management is often deceived into believing that security policies do not exist and that the organization is operating more effectively than it actually is. All organizations need to periodically review, test, and discard un-enforced and otherwise obsolete rules, controls, and procedures to avoid this false sense of security.

An alternative to periodic reviews is to specify a time limit for applying policies and standards and assign limited life span to mandatory controls, specifying when they should become effective and when they should be nullified or replaced—a technique generally referred to as sun setting. Computers are inherently vulnerable to a wide array of threats. It is generally worse to have no safeguards at all than to think that security is in place when it is not. This situation, known as negative value security, fosters complacency and diverts attention from the information assets, which are mistakenly presumed to be secure, making the information more attractive to hackers or more vulnerable to accidental loss. Information systems security policies are designed to address these threats.

D. Policy Development Responsibilities

Either the information systems security team or the IT policies and standards group under the direction of the information systems security team should be responsible for drafting appropriate policies and policy updates. As an alternative, some organizations assign the responsibility to a task group under the auspices of a management oversight committee. This is a common arrangement when the policies are being written or updated in conjunction with a re-organization or more drastic re-engineering of the information systems security team [1]. It is generally not a good idea to assign the policy-writing task to third-party consultants or use shelf ware since the style and form should be consistent with existing policies and should reflect the corporate culture.

It is important that the team drafting information systems security policies be sufficiently familiar with both current technologies and corporate culture to make intelligent decisions. Familiarity with current technologies requires an understanding of both the security capabilities and the limitations of technological solutions to protect the organization against threats [8]. Understanding the corporate culture additionally allows the policy development team to design an information systems security policy that can best ensure compliance.

E. Security Policy Violation

In order to realize the importance of a security policy, staff needs to be aware and fully understand the consequences of violating the policy, thereby exposing critical systems to a malicious attacker, or causing unintended damage to other companies worldwide. Violations should be handled accordingly; those who in one way or the other violate the security policy should be made aware that they may face being put through a "trial period", which involves also the limited use of some of the company information assets until they can show they are able to act in a secure manner while

using the corporate systems [8]. They should also be aware that in some (severe) cases they also may risk being fired or even prosecuted.

F. Importance of Policy

Information systems security policies are designed to inform the members of an organization of their obligatory responsibilities for protecting the information systems of their organization. These policies often specify the mechanisms through which these responsibilities can be performed. Information systems security policies also provide baselines to acquire, configure, and audit information systems for compliance with the policy (2008). Information systems security tools in the absence of policy, then, are of limited usefulness. Policies are significantly more important in a distributed computing environment than a centralized computing environment because of the increased challenge of constraining activity from a remote location.

Such policies must also be complete and clearly stated to reduce the amount of explanation. Policies should include general descriptions and identifiers for business units and functions rather than the names of individuals so that they can transcend organization changes. They should be confined to general concepts rather than specific controls. For example, a policy stating, "Each computer user must be authenticated by an acceptable method" is better than the more specific policy stating, "Each computer user must be authenticated by a six-character password" since the policy does not need to be changed should strong authentication tokens replace passwords.

Policy is also important in distributed computing environments as a means of establishing security discipline for a large, disparate group of users and business units that are generally only reached by formal communications and audit. This is particularly important when the organization relies heavily on contract or temporary personnel (2008). Policies should reflect the accepted practices of an organization yet take advantage of all practical methods for influencing behavior and disseminating information within the distributed computing environment.

G. Policy Acceptance

User awareness, education, and participation are key factors toward gaining policy acceptance. These factors can be promoted through information systems security marketing. The objective of security marketing is to inform, educate, and persuade the business units and users to engage in the secure computing practices outlined by policy, including providing process improvement suggestions to the management oversight committee. This can be achieved through security awareness programs.

In reality, neither external nor internal threats necessarily lead toward compliance. So it is essential that the security marketing team effectively convey the roles and responsibilities of the business units and users with respect to information systems security. Business units and users must understand that seemingly innocent computing behavior can have catastrophic effects.

Business units and users must also realize that information systems security policies are not infallible and unchangeable directives arbitrarily developed by an obscure and remote security policy development team. Business units must know that they have access to the policy development team so that they work together and improve existing policies.

In this manner, policies can evolve toward achieving a balance between information systems security and business practices that can allow the organization to optimally reach its business objectives. Since no policy can address every situation that might potentially arise in the future, it is important that there be a widespread realization of the underlying principles of the organization's information systems security policies [9]. This knowledge can serve as a guide in the undefined areas that stretch existing boundaries not originally envisioned by the policy development team.

III. SECURITY AWARENESS PROGRAM

The Security Awareness Program can be defined as one of the key factors for the successful implementation of an organizations-wide security policy. The main aim is to define and outline the specific role of each of the employees in the effort to secure critical company assets, as well as covering in detail each of the core elements pointed in the security policy. The program is aimed at generating an increased interest in the Information Security field in an easy to understand, yet effective way.

The Security Awareness Program is often divided into two parts, one being the 'awareness' section, the other, the 'training'. The purpose of awareness is to provide staff with a better understanding of security risks and the importance of security to the daily business procedures of the organization. The training part is aimed at covering a lot of potential security problems in detail, as well as introducing a set of easy to understand (and follow) rules to reduce the risk of possible problems.

A. Ethics in Security

We deal with the vast expanses of the Internet, a domain that knows no geographical boundaries or national or cultural lines. While on it, we interact with people from different parts of the world, with different values and beliefs. Apart from laws to regulate the on-goings of the Internet, its users also need to have a certain amount of responsibility and etiquette while using it. This does not apply only to Internet use, but also to general use of computer resources, hardware and software.

It is impossible to formulate laws to enforce all sorts of behaviors acceptable to society. Instead, society depends on ethics to build awareness of socially accepted behavior. Ethics are objective [5]. Unlike laws, they cannot be forced on individual [9]. In fact different individuals may have different ethical beliefs. The point however, is that some sort of social standards need to be set with regard to the use of computer resources. Unlike laws, ethics can be molded and modified to suit the situation much more easily [8]. Thus, it is the responsibility of groups, companies, organizations, service providers, and even countries to establish codes of ethical

behavior that people should strive to achieve and live by. As [5] asserts; in a utopian world, only ethics would be enough to have society function smoothly. With everyone striving to reach certain moral standards, there would be no need for laws. However, in the real world, ethics and laws have to operate hand in hand. The Internet was a highly useful medium and worked extraordinarily well as long as professional scientists and engineers dominated the user community.

The Internet began to experience problems when other groups of people (e.g., college students who were away from parental supervision for the first time in their lives, (people who were not professionals) joined the Internet, but did not honor the unwritten rules of etiquette for polite professionals. It is because of this change in the user community that the need for ethics in the computer world has increased many folds [6]. Today most organizations have written codes of ethics for its members to abide by. In a similar effort, the Computer Ethics Institute has developed its own ten commandments of computer ethics, which it believes computer users should abide by. However, encouraging users to abide by some kind of ethical standards need to be a collaborative effort.

B. Role of Ethics in the Awareness Approach

In [5], it argues that with regard to security guidelines, education should aim at the users internalizing the needs that drive the security guidelines. Thus, it is important that security guidelines are justified as normative claims, i.e., arguments and justifications are given. As a result, users may change their attitude and motivation towards the guidelines in the intended way, and attain prescriptive awareness of the subject of security, which is central target of the awareness approach. Persuasive communication, such as argumentation and justification, has been widely studied in the behavioral sciences, the results of which can be applied to the field of information security.

IV. ETHICS AND SECURITY MANAGEMENT

Ethics has a big influence on the behavior of individuals. If individuals (both users and security Managers) can be encouraged to engage in ethical thinking in the IS security context, this persuasive power can be utilized in IS security management [5].

Ethics is an important facet of comprehensive security of information systems. Research in ethics and information systems has been carried outside in the information security community. Typically, the hacking community has been arguing for the freedom of information. Security community has been opposing by arguing that system intrusion and hacking, even if no actual harm is caused, is unethical and criminal activity that one should not commit to, even if technically possible. The question rising from this conflict is how can the two groups claim they have a right to tell each other what is ethical and what is not [8]. The trend appears to be that the ethics approved by the security community is having the law enforcement.

Several attempts around the world are made to enforce proper behavior in the information society by juridical methods. From a stereotypic information security point of view hackers are seen as criminals, unaware of the results of their immoral activities making fun out of serious problems. Hacker community, on the other hand, sees information security staff as militants that do not respect the freedom of individual and information. These conflicts lead to the fundamental research questions within this paper: Is the ethics based foundation adequate, and how can it be made more feasible [7].

Comprehensive protection requires several types of technical and non-technical protection measures but technical measures are only considered regarding the feasibility of the proposed approach. Feasibility within current technology is a major requirement for a group based security model, and as will be shown, our proposal can be enforced by current secure group communication mechanisms.

A. Ethics and Information Security

Ethics in information system has been widely studied outside the information security community. Four major topics that ethics should address in information technology are:

Privacy: What information about one's self or one's associations must a person reveal to others, under what conditions and with what safeguards? What things can people keep to themselves and not be forced to reveal to others?

Accuracy: Who is responsible for authenticity, fidelity, and accuracy of information? Similarly, who is to be held accountable for errors in information and how is the injured party to be made whole?

Property: Who owns information? What are the just and fair prices for its exchange? Who owns channels, especially the airways, through which information is transmitted? How should access to this scare resource be allocated?

Accessibility: What information does a person or an organization has a right or a privilege to obtain, under which conditions and within what safeguards?

These four questions are the major concerns in the discussion of ethical dimensions of information security and hacking. The personal responsibility of individuals to respect these facets enters an essential role. If the approach towards society and networks is very different, groups cannot trust on the respect of other groups towards the facets. The situation becomes even more difficult when one group intentionally takes violations of the protection established to clarify these questions as a challenge and merit within their society [7].

V. MANAGEMENT COMMITMENT

Management commitment to security is essential to motivate information resource owners and users and to provide the visibility needed by the information systems security team to ensure the support of the business units. Because there are few natural motivations for security, other than actual loss experience, managerial commitment to information systems security is probably the most important factor in a successful security system [4]. In a distributed

computing environment, this commitment can be demonstrated to end-users and systems staff through the managers' own practices and performance reviews. Security training materials, guidelines, and computing practices should be signed off and approved by the authoritative local sources—typically managers who decide and issue rewards and penalties.

Management support of security provides the information systems security team with high visibility and fosters good rapport with high-level managers, particularly the senior managers of information intensive business units. Without the support of those individuals for the information systems security effort, their employees are less likely to support the effort. The best time to obtain visibility for information security is when a loss occurs [7]. If the loss occurs in the organization or business unit with the most resistance to information systems security or the greatest need for security, then the need for information systems security becomes more apparent. Emphasizing the negative effects of a loss experience on the whole organization can be one way of applying pressure to motivate all business units to improve security.

VI. CONCLUSIONS

The process of developing an effective information systems security policy is straightforward. Shaped by threats to an information system, the information systems security policy defines the objectives of the information system of an organization and outlines a strategy to achieve these stated objectives. It is important that senior management is committed to supporting the information security initiative. A policy-writing team, commissioned by a management oversight committee, should construct the policy to reflect the corporate culture. The security marketing team needs to inform and educate the organization about its security policies and persuade the users to engage in secure computing practices. Business units and users must know that they are an integral part of the information systems security process. Although straightforward, this process is not easily executed and the information systems security team must constantly strive to improve the process and provide the best defense against threats to the organization.

Conducting various security related contests from time to time not only helps measuring the security awareness level of staff, but also varies and innovates the educational process. Password cracking contests are a good example; they contestants are faced with the challenge of cracking a file that has been protected by a password chosen by a fellow contestant, with the idea of finding/eradicating weak passwords. Upon conclusion of the contest a discussion is started on how the password was cracked, what makes it a weak password (if that was the case), etc. Most staff are usually interested in such activities, and most of them will do their best to use hard to crack passwords following the recommendations on the process of creating strong passwords from the Security Awareness Course.

REFERENCES

[1] Amnesty International (2008). Amnesty International Report 2008. The State of the World's Human Rights. Online: http://thereport.amnesty.org/document/101 [14.09.2008].

[2] Woodard, E (2010). Network Security: Policies & Procedures, Technical Support, Vol. **8** (11) http://www.naspa.com/PDF/2010/1100

[3] Wood, C. C. (2009). Information Security Policies Made Easy, Version 7. Baseline Software, Inc.

[4] Anderson, R. J. (2002). Unsettling Parallels Between Security and the Environment. Workshop on the Economics of Information Security 2002. Online: http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/37.txt

[5] Iandolo, R. (2008). "Acceptable Use Policy Document." SANS Institute. http://www.sans.org/infosecFAQ/policy/accept_use.htm

[6] Schneier, B. (2000). Secret and Lies: Digital Security in a Networked World. Wiley Computer Publishing.

[7] BITS (2009). BITS Framework for Managing Technology Risk for IT Service Provider Relationships (Second ed.). Online: http://www.bits.org/downloads/Publications%20Page/bits2003framework.pdf

[8] Morris F. (2001). "Enhancing Information systems security in an academic organization". In Proceedings of 7th International Conference of European University Information Systems (EUNIS), Berlin, Germany, 2001. Humboldt University, 2001; pp 92-94. [SZ01]

[9] Boeing (2008). Statistical Summary of Commercial Jet Aircraft Accidents. Worldwide operations. 1959-2007. Online:http://www.boeing.com/news/techissues/pdf/statsum.pdf