International Journal of Soft Computing 2 (3): 408-410, 2007

Information Security Policy: Relevance, Creation and Enforcement

A.J. Jegede, G.I.O. Aimufua and H.O. Salami
Department of Mathematical Sciences, Nasarawa State University, Keffi, Nigeria

Abstract: Electronic information and the means for transmitting and processing it are now indispensable to many areas of operations in organizations. The power and convenience of information technology is, however, counterbalanced by the wide range of threats to the security of electronic information. This study explores the concept and relevance of security as it relates to electronic information systems. It also sets out the background to preparing an information security policy as well as the strategies required for implementing and enforcing such policy.

Key words: Auditing, enforcement, information, information security, security, security policy

INTRODUCTION

Security is defined as something that provides safety or freedom from danger or anxiety (Hornby, 2000). This definition encompasses a set of measures taken to guide against theft, attack, crime and espionage. Thus, information security implies the quality or state of information being secured. That is, when information is free from exposure to any of the above-mentioned dangers and acting so as to make safe against adverse contingencies.

The growing use of a reliance on computers and computer-based systems worldwide has resulted in legitimate concern for security. According to Milenkovic (1992), the use of computer has become pervasive in business, government, military and even at home. This assertion is found to be very true because large amounts of vital and sensitive data are increasingly becoming entrusted to and stored in computers. Some of the systems today that rely on computers include transportation systems; personal and corporate financial records and systems; credit card processing systems; Automatic Teller Machines (ATMs); telecommunication systems, air traffic control systems, systems responsible for storing and transporting healthcare data, power systems, generic payment processing systems and ticketing systems (Anonymous, 2001).

Concept of security policy: Milenkovic (1992) defined security policies as procedures and processes that specify:

- How data can enter or exit the system.
- Who is authorized to access what information and under what conditions?
- What are the permissible flows of data within the system?

Basically, computer related security policies could either be discretionary access control or mandatory access control (Jegede, 2004). Discretionary access control allows policies to be defined by the owner of computer resources (hardware and software), who may pass access rights to users. Mandatory access control scheme, on the other hand, classifies users according to the level of authority or clearance. Here, computer resources are classified into security classes according to the level of confidentiality and strict rules are defined regarding which level of user clearance is required for accessing the resource of a specific class.

Security policies are often guided by the age-old principles of:

- Least privileged, which requires that each user be allowed access only to the resources essential for completing the task that the user is authorized to carry out.
- Separation of duties: This principle requires that twoor more people with conflicting interests carry out the set of operations that can put an organization at risk.
- Rotation in roles: The effectiveness of this principle is based on the fact that sensitive operations should not be permanently entrusted to the same personnel. Some amount of rotation is more likely to uncover wrongdoings.

The choice of an adequate security for a given enterprise and for specific resources therein is usually a

Corresponding Author: A.J. Jegede, Department of Mathematical Sciences, Nasarawa State University, Keffi, Nigeria

trade-off between the perceived risk of exposure, the potential loss due to the loss or exposure of information and the cost of providing a specific level of security. The process consists of risk assessment, which includes increased cost of equipment, personnel and reduced performance due to security measures.

RELEVANCE OF INFORMATION SECURITY POLICIES

To secure enterprise environment, it is imperative to have a set of security policies that specify what is required in terms of security and protection. The reasons for adopting a formal policy on the security of electronic information are two-fold:

- To provide a framework for best operational practice, so that the establishment is able to minimize risk and respond effectively to any security incidents which may occur.
- To ensure that the establishment complies with relevant legislation in this area.

A security policy provides a context within which to define roles and responsibilities with respect to data (and information) security, to formulate and justify any regulations, which are felt to be needed and make explicit the organizations attitude to any action, which threaten the security of information assets (Developing an Information Security Policy). A security policy is highly essential to the safety of information in an enterprise as it outlines what actions or risk management procedures must be covered in order to protect corporate assets.

Since electronic information is at risk for a whole variety of reasons: natural disasters, failure of man-made equipment and services and accidental as well as malicious acts by human beings, it is therefore imperative to put a clear, comprehensive and realistic policy in place so that the safety of information in an enterprise can be guaranteed.

CREATING A SECURITY POLICY

General principles: There are a number of possible routes available when creating information security policies ranging from off the shelf purchase, to carefully crafting every clause and sentence. The most effective way, according to Computer Security Policies Directory, is to procure a set of pre-written policies and then tailor them as necessary to meet specific organization needs. Irrespective of the approach that is adopted, we recommend that a policy must strike a balance between privileges and responsibilities. That is, making information and resources more freely available to members of an organization arguably places more onuses on those members to behave responsibly.

On the human front, the policy must define what behaviour is and is not allowed, by whom and in what circumstances. On the practical and operational front, the policy should provide the context for a supporting set of guidelines and procedures, which will establish at a detailed level, how security is implemented for all information systems concerned. Overall, the policy must define the role that information security plays in supporting the mission and goals of the organization.

Structuring a policy document: A number of ways to structure an information security policy document of this kind has been identified. The best approach, however, is for the high-level policy document to be short and easily understood. It should deal only with the key essentials, for example, its purpose; its scope; definition of security responsibilities; procedures to be followed in case of emergency and possible sanctions in the event of a deliberate contravention of the policy. More detailed aspects of security policy can be addressed where necessary, by making reference to supplementary documents dealing with specific issues. Such supplementary documents may include additional, more focused, statements of policy, which apply in particular circumstances and also guidelines and procedures describing day-to-day security practice.

Although the high-level policy document should be reviewed periodically to ensure that it remains in step with the evolving needs of the organization, it is very important to frame it in a way that is relatively independent of particular technologies so that the policy does not date rapidly because of technological advancement.

Finally, it is essential that the policy is clearly and comprehensively, written and above all, that it is realistic; that is, the policy is capable of practical implementation and that any sanction is appropriate and can be enforced.

ENFORCEMENT OF SECURITY POLICY

Having a security policy document is not enough; the contents must be implemented for it to be effective. The policy should be backed up by an implementation plan which sets the desired security level for all information systems of importance and the consequent measures for achieving these security goals. The fundamental question, however, is how to deploy the policies; that is, how to deliver them. This is critical, as

undelivered or badly delivered policies might as well not exist. The most dynamic and direct method is to deliver the policies directly to the user's desktop. This has a lot of benefits, including:

- Instant availability for the user.
- Familiar navigation interface; for example using windows, search facilities, etc.
- The potential to use the power of a PC to make the experience richer and more productive for the user.

Without enforcement, a security policy is likely to be followed for a short time after implementation, but generally falls into a state of disuse. To enforce a security policy, we suggest that organizations exploit the binding nature of a written contract. Employees (and other information systems users) should read and agree to the security policy by signing it.

Auditing of the environment and its users for compliance with the security policies is another suggested approach to enforcement. Farmer has identified two general types of audits-notified or scheduled audit and blind audit. Scheduled audits are announced to the users (employees) and help to establish compliance where it is otherwise lacking. Inspection of this nature often involves several stages. The first occurs at the technical level, where in the systems, network and facilities are analyzed for their security components, to ensure that they meet the requirement of the security policy. A final stage is the analysis of the auditing methods to ensure they gather the appropriate information and meet the goals of the audit.

Blind audits are audits that are randomly and periodically scheduled without any notification to those being audited. They are useful to establish the constant security awareness needed to maintain security as the organization flourishes. Blind audits come in the form of simulated attacks or planned scenarios to exemplify a particular security practice. This aspect of audit might include attempts to enter the facility, acquisition of passwords or access keys and attempts to gather private information about the organization. The response of the employee and the ability of the auditor to gather this information demonstrate the level of awareness and the level of compliance with current security policies. A major Advantage of this approach is that the knowledge that an audit could occur at anytime, without notification, forces users to incorporate security awareness and practices into their daily routines.

CONCLUSION

In summary, organizations are strongly encouraged to adopt a recognized methodology for developing their security policies and plans. Moreover, the policies should strike a good balance between confidentially, availability and operational costs. This is because extensive security measures can increase cost and restrict the usefulness, user friendliness and performance of information systems. It is therefore recommended that the policies strike a good balance between availability and confidentiality so that what is gained in security is not lost in performance.

Training is also necessary to enable employees appreciate the relevance and benefits of security policies in order to avoid deliberate or accidental circumvention of such policies.

REFERENCES

Anonymous, 2001. Maximum Security. (3rd Edn.), Indianapolis: Sams Publishing Company.

Developing an Information Security Policy. JISC senior Management Briefing Paper 13. http://www.jisc.ac.uk/index.cfm?name=pub-smbp-infosec.

Farmer, Improving the Security of your Site by Breaking Into It. http://www. alw. nih. gov/security/Docs/admin-guide-to-cracking.101.html.

Hornby, A.S., 2000. Oxford Advanced Learners Dictionary of Current English. (6th Edn.), Oxford University Press. The Information Security Policies/Computer Security Policies Directory. http://wwwinformation-securty-policies-and-standards.com.

Jegede, A.J., 2004. A Specification of an Application Gateway for Client/Server Systems. University of Ibadan: M.Sc, dissertation.

Milenkovic, M., 1992. Operating Systems: Concepts and Design. (2nd Edn.), Singapore: McGraw-Hill.

The Information Security Policies/Computer Security Policies Directory. http: // www information-securty -policies-and-standards.com.