THE KEY ROLE OF INFORMATION SECURITY IN E-COMMERCE[1]

A. Sanaye'i, Ph.D.
Associate Professor at Faculty of Administrative Sciences & Economic
University of Isfahan, I. R. of Iran
email: sanayei110@yahoo.com

Abstract - Information security is one of the most important enterprise assets. For any organization, information is valuable and should be appropriately protected. Also, security is to combine systems, operations, and internal controls to ensure the integrity and confidentiality of data and operation procedures in an organization. Knowing the fact that with serious threat of unauthorized users on the Internet, information security is facing unprecedented challenges, and effective information security management is one of the major concerns. Moreover, the field of computer and information security focuses on designing measures that can enforce security policies, especially in the presence of malicious attack. On the other hand, security in E-commerce generally, employs procedures such as authentication, ensuring confidentiality, and use of cryptography to communicate over an open system. In this paper, we will discuss the security in cyberspace and recommend some suggestion for application of security in e-commerce.

Keywords - Information Security, E-Commerce, Cyberspace, Developing Countries, Security Risks.

INTRODUCTION

Security is a major issue for computer users and system administrators. Whether to protect confidential information in individual files, lock a computer system to unauthorized users, control access to an intranet or extranet, or conduct business on the Internet, one needs to determine an appropriate level of security and effective means to achieve the objective.

On the other hand, most applications rely on passwords, cards, personal identification numbers and keys to access restricted information or confidential files. But passwords, cards, personal identification numbers, and keys can be forgotten, stolen, forged, lost or given away [1].

Moreover, the major goal of information security is mainly to detect and prevent the unauthorized acts of computer users. And the broad objectives of a computer security policy are to ensure the data confidentiality, integrity, and availability within information systems (e.g. ISO/IEC 17799, 2000 that gives a different scope for information security management that includes: Information security policy and assessment, information security organization and responsibility, and personal security management). Information security

issues cover information security policy, risk analysis, risk management, contingency planning and disaster recovery. Information security management contents also vary with different researchers and institutions. For instance, according to Tudor (2001), as stated in [11], there are five components for any information security architecture: Security organization & infrastructure, security policy & standard procedures, security baselines, security awareness, and compliance.

INFORMATION SECURITY & ITS POLICY

There has not been consistent security policy theory yet. However, several scholars declare that information security could be achieved through the establishment, implementation, and maintenance of information security policy. For example, Kabay [8] pointed out that the establishment of information security policy should include five procedures, which are:

1. to assess and persuade top management
2. to analyze information security requirements
3. to form and draft a policy
4. to implement the policy, and
5. to maintain this policy.

The information security policy life cycle proposed by Rees, as stated in [12], addressed four parts:

1. policy assessment
2. risk assessment
3. policy development and requirements definition, and
4. review trends and operation management.

The e-policy proposed by Flynn [4] covers: comprehensive e-audit; e-risk management policy and computer security policy, cyber insurance policy; e-mail policy; Internet policy and software policy. To sum up, information security policy aims at planning information security requirements, forming consensus in an organization, drafting and implementing a policy, and reviewing the policy on a regular basis in order to meet the demands of organizational security requirements. This theory could be expressed in terms of three functions below [4]:

1. Information security = f (information security policy)
2. Information security policy = f (establishment, implementation, and maintenance of information security policy)
3. Information security establishment = f (organizational security requirements)

Information security in network logical barriers and the Internet logical barriers, required to minimize exposure from the Internet, or any other external network, are just one component of the total information security infrastructure, and they should not be

given high priority to the detriment of the other elements.

While information security exposures are increased when outside users access a network, managers concerned with security should be aware that sound security practices are essential with or without access by external parties.

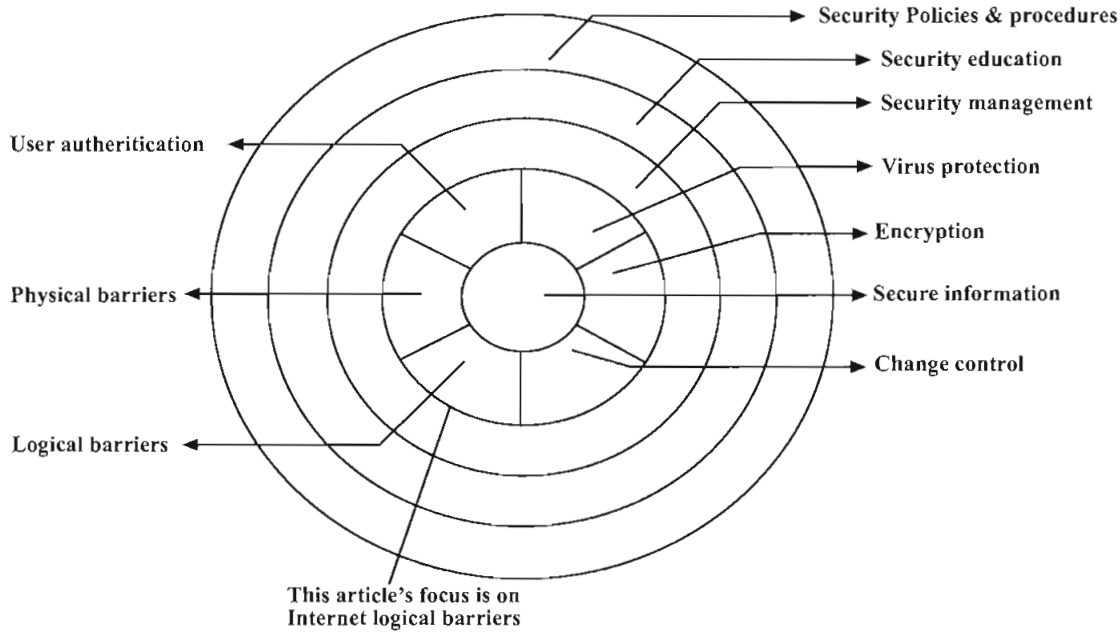

Figure 1: Information security protection [3].

While cryptography can provide a good shield to protect the transmission of data, it does not protect a network from software intrusions – the large problem of virus attacks. The virus problem has developed so rapidly that it has created an industry to counter it and try to keep businesses clean of infection – the anti-virus industry. The definition of what a virus is can be tricky in a networked environment. Virus-L is a moderated listserv established on the Internet that promotes the communication of information about viruses and details a great deal of information in its Frequently Asked Questions (FAQ) manual. Its FAQ, available on the Internet, describes a virus as:

According to Fred Cohen's definition, [2] a COMPUTER VIRUS is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself. Note that the program does not have to perform outright damage (such as deleting or corrupting files) in order to be called a "virus"... Many people use the term loosely to cover any sort of program that tries to hide its (malicious) function and tries to spread onto as many computers as possible...be aware that what constitutes a "program" for a virus to infect may include a lot more than is at first obvious – do not assume too much about what a virus can or cannot do. A good security system will either have built in, or will work with, a well-built anti-virus program that allows easy upgrades of virus information. It should also include the ability to control virus protection from the network server and not let individuals in the company decide

how they want to use anti-virus programs [9].

The anti-virus industry is extremely large and could have papers upon papers about its subject. There must be a strong commitment by the company to ensure that anti-virus protection and configuration is in place and is an integral piece of the security.

Risk assessment is an essential element of risk management. All elements of the risk management cycle are important, risk assessments provide the foundation for other elements of the cycle. In particular, risk assessments provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Since risks and threats change over time, it is important that organizations periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected. This continuing cycle of activity, including risk assessment, is illustrated in the following depiction of the risk management cycle [5].

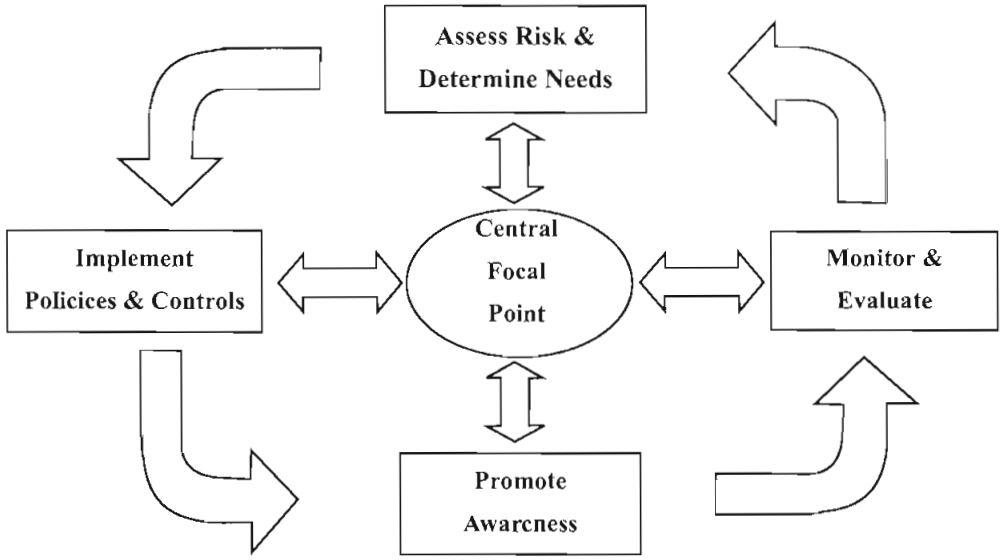

Figure 2: Risk management cycle.

E-COMMERCE SECURITY COMPONENTS & ITS STRATEGIES

The E-commerce security strategies deal with two issues: Protecting the integrity of the business network and its internal systems with accomplishing transaction security between the customer and the business. The main tool businesses use to protect their internal network is the firewall. A firewall is a hardware and software system that allows only those external users with specific characteristics to access a protected network. The original design was supposed to allow only specific services (e.g., email, web access) between the Internet and the internal network. The firewall has now become the main point of defense in the business security architecture. However, firewalls comprise a small part of the business security infrastructure. There are hacker tools such as SMTPTunnel and ICMPTunnel that allow hackers to pass information through the allowed ports. The "ILOVEYOU" virus successfully penetrated firewalled networks because inbound and outbound email is

allowed to pass through the firewall. The Code Red and NIMDA worms passed through firewalls because they accessed systems through the standard WEB server ports. Transaction security is critical to bolstering consumer confidence in a particular e-commerce site. Transaction security depends on the organization's ability to ensure privacy, authenticity, integrity, availability and the blocking of unwanted intrusions. Transaction privacy can be threatened by unauthorized network monitoring by software devices called sniffer programs. These programs are most likely found at the endpoints of the network connection. There are a number of defenses against this threat such as encryption and switched network topologies. Transaction confidentiality requires the removal of any trace of the actual transaction data from intermediate sites. Records of its passage are a different thing and are required to verify that the transaction actually took place. Intermediate nodes that handle the transaction data must not retain it except during the actual relaying of the data. Encryption is the most common method of ensuring confidentiality. Transaction integrity requires methods that prevent the transactions from being modified in any way while it is in transit to or from the customer. Error checking codes are examples of such a method.

Encryption techniques such as secret-key, public-key and digital signatures are the most common methods of ensuring transaction privacy, confidentiality and integrity. The common weakness of these techniques is that they depend on the security of the endpoint systems to protect the keys from modification or misuse.

CHALLENGES ASSOCIATED & INFORMATION SECURITY RISKS

Reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk actors are often more limited and because risk factors are constantly changing. For example, data are limited on risk factors, such as the likelihood of a sophisticated hacker attack (see Figure 3), and the costs of damage, loss, or disruption caused by events that exploit security weaknesses. Some costs, such as loss of customer confidence or disclosure of sensitive information are inherently difficult to quantify. Although the cost of the hardware and software needed to strengthen controls may be known, it is often not possible to precisely estimate the related indirect costs, such as the possible loss of productivity that may result when new controls are implemented. And 8 GAO/AIMD-00-33 Information Security Risk Assessment, even if precise information were available, it would soon be out of date due to fast-paced changes in technology and factors such as improvements in tools available to would-be intruders [11]. This lack of reliable and current data often precludes precise determinations of which information security risks are the most significant and comparisons of which are the most cost-effective. Because of these limitations, it is important that organizations identify and employ methods that efficiently achieve the benefits of risk assessment while avoiding costly attempts to develop

seemingly precise results that are of questionable reliability [7].

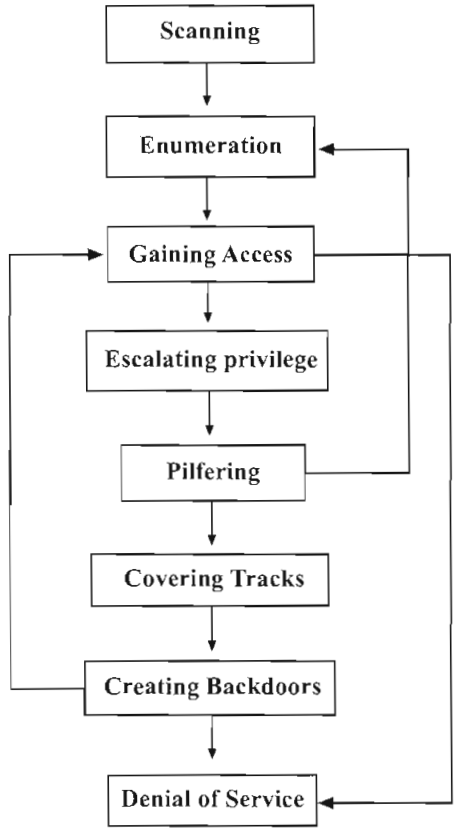

Figure 3: Anatomy of hacking [11].

To assist agencies in meeting this challenge and to supplement our May 1998 guide on information security management, we studied the practices of four organizations that had institutionalized practical risk assessment methods. We identified these organizations based on recommendations from government and private sector sources [10].

These sources recommended over 30 private and public sector organizations that were known to have strong security programs or to be actively pursuing improved risk assessment practices. The four organizations included a multinational oil company, a financial services company, a regulatory organization, and a computer hardware and software company. This guide describes the factors that these organizations considered critical to the success of their risk assessment processes and the benefits they cited as a result of these practices. In addition, it provides a description of the procedures they followed and examples of the tools they used to facilitate the process. The organizations we selected had chosen risk assessment methods and developed tools that were relatively simple and, for the most part, qualitative in nature. However, one organization used a combination of qualitative and quantitative methods. In some cases, agencies may find that it is more appropriate to use more detailed, quantitative methods to assess the risks associated with certain aspects of their computerized operations. However, incorporating the critical success factors that we identified is likely to make any type of methodology more effective.

INFORMATION SECURITY MANAGEMENT STANDARDS

The Information Security Management Standards, first published by the British Standards Institute in 1995 and recently adopted by the Australian and New Zealand Standards Association, provide an authoritative statement on the organizational need for information security, and the procedures to be adopted for baseline security. They can, thus, represent a major step forward for the security officer. If used and interpreted effectively they can help to overcome some of the inherent problems identified above. These standards require a careful interpretation for current organizational environments, since on first reading they appear to be biased towards large computer centers.

Nevertheless, they do provide an important authoritative statement for senior management, and extensive checklists of security measures. Security officers would be well advised to develop local guidelines, based on an informed interpretation of the standards, customized to the organization, and then submit an initial report for senior management. Such a report should detail the extent to which the organizational level of information security management is, or is not, consistent with the guidelines. The recommendations in the standards are, as indicated above, geared to a baseline level of security. Once the requirements at this level have been addressed, the local scene should be reviewed to determine if the level of perceived risk justifies a more extensive study and more stringent countermeasures. Even if such a study is not deemed necessary, the security officer may well be required, at some future time, to satisfy external auditors that the organizational level of information security is in conformance with internal or external requirements. Such risk analysis and/or security audits will involve documentation of the current organizational security scenario and this is likely to be a major task when undertaken on the first occasion. The major problem is that the task is likely to be equally demanding on any future occasion; if security audits checking conformance to standards or external imposed requirements become regular events, then some careful forethought is required on the manner in which the security officer records the local scene. Commonly existing organizational documentation, even for large corporate bodies, is not in a form suitable for the security officer's purpose. In many cases the information resides in scattered filing cabinets or hard disks; often it is part of the oral history of the corporation. When the information is collected from its various sources, it will be difficult to glean security-relevant features from a vast mass of operational/administrative procedures and guidelines. Much of the information will be outdated. When the security features have been gleaned then there will be a major task of cross-referencing material from its various sources. The task of data collection is likely to be so demanding, and the resultant set of refined security information so incomplete, that the results of any risk studies may be viewed with skepticism [6].

It is suggested in this paper that the problem described above arises because the data collection task is normally considered the first phase of a security audit or risk analysis. It is recommended that the security officer develops and maintains a security model of the organization, so that it is available when required for future risk analyses and security audits. The maintenance of the model should, as far as possible, be organized in such a way that changes in the organization that impact on security should be captured and included in the model as a matter of routine [11].

With such a model in existence the security officer is in a less hazardous situation. The security officer can at least demonstrate to external audits that he/she has a clear understanding of the current state of information security, and its potential weak points. If he/she is wise he/she will also be able to produce records of his/her recommendations to senior management and their responses. As was stated above, in most organizations, current documentation does not provide the model required by the security officer. Given the rate of change of information processing systems it is unlikely that paper documentation can easily handle model updates and cross-referencing. This paper describes a model of organizational security suitable for the proposed purpose and indicates how it may be used to demonstrate conformance with current standards.

CONCLUSIONS

There can be no conclusive directives in computer security because of its nature and its constant dynamic re-inventing of itself that makes it a difficult field to pin down. Computer security is the final frontier because there is no end to the possibilities of attacks and counterattacks. It always forces security personnel to change their definitions of it, while they try to manage security risk. Computer security is and always will be the tool that allows safe communication in the future.

Furthermore, knowing the fact that, there are several reasons for the recent emphasis on the key role of information security such as global trading, online and real-time trading, availability of reliable security packages, and change in attitude toward security in e-commerce is essential.

In this paper, we can suggest for any new enterprise in a developing country to do the following for a better use of information security application in e-commerce as follows:

Create an authentication for a better process of identifying the user for a specific system, and having denial of service for preventing third parties from using the infrastructure, using encryption for coding the messages between computers, establishing firewalls between the net works, monitoring, and last but not least to create a privacy for user availability to use certain information in secure space.

ENDNOTE

1. This paper was presented by Prof. Dr. Ali Sanayei at ICGeS 2006, International Global E-Security Conference, University of East London, UK.

REFERENCES

[1] Awad, E., *E-Commerce from Vision to Fulfillment*. NY, Prentice Hall, 2002.

[2] Cohen, F., *A Short Course on Computer Viruses*. Pittsburg, ASP Press, 1990.

[3] Doddrell, G. R., "Information Security and the Internet Research." *Electronic Networking Applications and Policy*, Vol. 6, No. 1, pp. 5-9, 1996.

[4] Flynn, P., *CAS-CAT-Project*. Melborn, 2001.

[5] Forcht, K. A. and Fore III Richard, E., "Security Issues and Concerns with the Internet." *Internet Research: Electronic Networking Applications and Policy*, Vol. 5, No. 3, pp. 23–31, 1995.

[6] Harlow, J., "Security Policy-an Individual View." *Victim Information and Notification Everyday*, Vol. 100, No. 123, pp. 17-32, 2002.

[7] Hawkins, S., et al., "Awareness and Challenges of Internet Security." *Information Management & Computer Security,* Vol. 8, No. 3, pp. 131-143, 2000.

[8] Kabay, *Computer Security: Anatomy of Usability Disaster*. UK, 1996.

[9] Kesh, S., et al., "A Framework for Analyzing E-Commerce Security." *Information Management & Computer Security*, Vol. 10, No. 4, pp.149-158, 2002.

[10] Mitchell, R. C., et al., "Corporate Information Security Management." *New Library World,* Vol. 100, No. 1150, pp. 213-227, 1999.

[11] Sanderson, E. and Forcht, K. A., "Information Security in Business Environments." *Information Management & Computer Security,* Vol. 4, No. 1, pp.32-37, 1996.

[12] Smith, A. D., "E-Security Issues and Policy Development in an Information-Sharing and Networked Environment." *Aslib Proceedings: New Information Perspectives*, Vol. 56, No. 5, pp. 272-285, 2004.