A SURVEY OF INFORMATION SECURITY

Nancy Tsai
Management Information Science Department
California State University, Sacramento, USA
Tel: (916) 278-7121
Fax: (916) 278-6757
tsain@csus.edu

ABSTRACT

The current global network infrastructure of the e-business has brought the information security systems of the organization to a new frontier. A detrimental destruction to an organization's information system can be done electronically through the telecommunication of the Internet without the time restriction and from everywhere in the universe. Therefore, the security of protecting the information resources has become an essential management issue in any organization. This research attempts to determine how organizations are currently viewing the objectives of their information security systems and to describe their relative success with the use of the available counter measurements against the traditional thieves and electronic crimes using a survey questionnaire.

KEYWORD: security, information system

INTRODUCTION

In the last two decades of the 20th century, the affordable and powerful computer hardware and software along with the advanced telecommunication technology have laid a solid foundation for the emerging and popularity of the Internet. The individual and organization have quickly adopted the Internet as a communication tool for transmitting the data, information and service since it is fast, simple, and convenience without the limitation of distance and time.

The organization promptly understands the benefits offered by the Internet and establishes a new sales and supply channel named e-business to gain the competitive edge. The function of the e-business is to electronically connect the organization with its client and supplier forming a global business partnership network using the capability of the Internet. Consequently, the establishment of the e-business has changes the surrounding conditions of an organization's information system in term of two aspects. First, the closed private network becomes an open public network within the community of the organization. Second, the proprietary computing architecture has been replaced by a standard and distributed client/server computing architecture in the organization that can be comprehended and penetrated by any professional in the related fields.

Through the Internet, any threat or terrorism is only a click away that can significantly damage the data and paralyze the information system of the organization. In addition, the Transmission Control

Protocol and Internet protocol (TCP/IP) required to transmit the information over the Internet was developed without the security consideration [1]. Not only the identification of the sender and receiver addresses, but also the transmission data can be easily intercepted, interpreted, and altered under the fingertip of an unauthorized information hacker if no additional security measure for the transmission is used.

This global network infrastructure of the e-business has brought the information security systems of the organization to a new frontier. The risk of theft, loss of privacy, and the detrimental destruction to the data and system within the organization can be done electronically through the Internet communication without time restriction and from everywhere in the universe.

Therefore, a research study was considered to be necessary to attempt to determine how organizations are currently viewing the objectives of their information security systems and to describe their relative success with the use of the available counter measurements against the traditional thieves and current electronic crimes. A questionnaire was constructed to collect data about how the information security is being developed in organizations and to learn what types of results are being achieved. This paper was written to present the findings of this research effort for the information of MIS practitioners and MIS academics.

The paper begins with an overview of what is believed to be the major attributes including objectives, resources, threats, and counter measurements that form the information security system strategy. Next, the research that was performed is described. Findings are presented which describe the extent and the manner in which the various threats are being encountered and the counter measurements are being implemented by organizations. Evaluations were developed to express the degree of security objectives being achieved and the various counter measurements used to protect information system assets.

OVERVIEW OF THE INFORMATION SECURITY SYSTEM ATTRIBUTES

The fundamental attributes in analyzing and dealing an organizational information security system can be identified as objective, resource, threat, and countermeasure. The objectives are a set of benchmarks to measure the effectiveness of the implemented security system. They also serve as guidelines to determine the required counter measurements to protect the information assets from the physical and electronic threats.

Objective

The descriptions of the seven most common objectives [2, 3] to implement an information security system in the organization are presented as below:

(1) Confidentiality: to prevent the disclosure or exposure of the data and information to the unauthorized individual or system;
(2) Integrity: to maintain the data and information at a state of currency, consistency and accuracy;
(3) Availability: to provide the service at an acceptable level of quality without any interference and obstruction;

(4) Authentication: to verify the real identity of the information system user;
(5) Authorization: to control and manage the right of individual and system to access the data and information;
(6) Accountability: to assure the non-repudiation of the communication between the message sender and information receiver; and
(7) Privacy: to guard against unauthorized collection, storing, distribution, and usage of the personal information for preserving the right of individual.

Resource

The resources of the organizational information system can be classified as physical assets, processing functions, data and information. The physical assets include computer hardware, network equipment, system software, middleware, application software, and other physical facilities to house the information systems. The processing functions are the logistic operations to gather and transform the input data to useful output information for management decision making. The data and information composes the database where stores the interrelated data files as a central depository and allows the organization to search the information for its competitive opportunities.

Threat

In general, the sources of all threats to a computerized information system can be grouped into five major categories that include accidental, deliberate, Mother Nature, technical failure, and management failure. The accidental treats are generated by the careless operation behaviors of information system staff. The deliberate threats are produced by the disgruntled internal employees within the organization or by the external malicious hackers located in the universe. The Mother Nature can create catastrophes to a serious destruction to the data and information without any warning sign. The technical failure is due to the malfunction of the hardware, bugs in the software, and disruption of the telecommunication network. The management failure comes from the incomplete or missing security policy and procedure defined by the organization to protect the information systems.

The consequences of the actual threats to a computerized information system include corrupted operations, compromised systems, loss of assets, loss of service, loss of data integrity, loss of information privacy, loss of customer trust, loss of sales, and loss of profit. These consequences could cause severe damage ranging from the process of the information systems to the survival of the organization only because there are flaws in the information security systems to permit the unauthorized access, modification, use, and destruction of hardware, software, data, or network resources.

It becomes essential to have certain predetermined mechanism included in the information security system to identify and report the threat as soon as it occurs for two major reasons. First, the organization can immediately conduct the damage control to minimize the negative impacts on the routine business operations. Second, the organization can use the reported incident to strengthen its information security system by designing a set of countermeasure to prevent the future reoccurrence of the same threat.

The threat incident identification mechanism includes audit logs, detection devices, monitoring tools, internal incident reporting process, external incident reporting process, advance warning by authority, advance warning by other entity, denial of service, data/information asset corruption, system downtime, termination of communication mechanism. Most of these mechanisms could be either manual process or software program to monitor and analyze the routine usage logs of the information system resources. They detect and provide a real time warning regarding to the abnormal activity in an unauthorized manner. The advance warning by authority and advance warning by other entity are related to the official government's announcement about the possible disaster caused by the Mother Nature or national terrorisms.

Counter Measure

The countermeasure is a set of controls or approaches to prevent damage generated by any potential threat to the organizational information system resources. The organization can implement three layers of controls including, administration layer, technical layer, and operational layer to fully secure its information system resources from the accidental or deliberated events.

The administration level establishes a management framework of security policy and procedure for the entire organization. It composes of the security policy for defining the information system security standard and guideline, the risk management for determining the counter measures to protect the information resources in terms of cost benefit analysis and the recovery plan for recovering the data and information system from any human incident and the Mother Nature attack.

The technical level utilizes the advanced computer hardware and software technologies to protect the organization's private intranet and telecommunication. That includes the authorization and authentication for system access control, data encryption and decryption for transmission confidentiality, digital signature and electronic certificate for increasing trust and accountability, network monitoring program for operation availability and security, and the firewall for blocking intruders to the organization's intranet.

The operational level utilizes the physical devices established in the technical level to properly monitor the routine performance of the environmental and access controls for avoiding the malicious vandalism or theft. It also follows the security standards and guidelines developed in the administration level to perform the personnel management and inventory control for documenting the information system resources.

THE RESEARCH

An extensive questionnaire (10 pages) was developed to survey computer information system users about their approaches to the current information system security. The primary purpose of the research was to collect the data about the adopted management infrastructure, the embraced objectives, the resources to be protected, the threats encountered, the counter measures implemented, and the results being achieved of the information security systems in the current global telecommunication environment.

Methodology

Questionnaires were sent to the top level information management staff, both in the private and public sectors, throughout the United States. The survey target was the chief information officer of the state government offices, local government offices, and corporations. The on line state publication directory and distribution list of the California Multiple Award Schedule were used to randomly select the organizations to which to send the questionnaires.

326 questionnaires were sent out to the organizations via U.S. Postal Service. 137 emails were sent out using an academic organization address to request the organizations answering the questionnaire that was posted on a college related web site. Unfortunately there is a zero response rate via the combination of the email and the Internet. Only twenty eight usable questionnaires via U.S. Postal Service (about nine percent return rate) were returned and provided the data which are presented and interpreted in this paper.

Characteristic	Low Value	Median Value	Average Value	High Value
Annual Revenue (millions)	1.3	130	1,189	175,000
Total Employees	6	590	7,458	60,000
IT Employee (percentage of total employee)	0.01	0.05	0.36	1.00
E-business Employee (percentage of IT employee)	0	0.03	0.08	0.60

Table 1 Characteristics of Industry Sample

The profile of the diverse organizations which responded to the survey is summarized in Table 1. The purpose of this research was set to collect detailed data about how an organization deploys information system security. Because of the volume of data collected, only a summary of the more important results will be presented in this paper.

The Findings

The summarized data have been grouped to illustrate the involvement of the management personnel, objectives of the information security system, the type of resources to be protected, the major threats encountered, and the counter measures implemented in terms of administration, technology, and operation to against the threats. A brief discussion and interpretation of the more significant results is, also provided. It should be noted that some responders did not complete all the appropriate section of the questionnaire.

In the questionnaire, responders were asked to check the type of executive staff involved in the decision making process for the information systems security

within their organizations. Table 2 indicates that the chief executive officer, privacy officer, and information security officer have been heavily engaged in the organizational security decisions. Clearly, the security is now regarded as one of the most important routine operational issues and it needs a top down uniform strategy to guard the information and its physical resources for the entire organization. The results also reveal that the chief financial officer is the least executive manager for the security decision. This aligns with the facts that the existence of the security systems and its funding decisions can not be evaluated based on the financial return rate generated by the investment.

Management Personnel	Number Reporting	Percentage Value
Chief Executive Officer	16	0.57
Chief Financial Officer	5	0.18
Chief Security Officer	7	0.32
Information Security Officer	9	0.43
Privacy Officer	12	0.11

Table 2 Management Personnel Involvement in Security Decisions (n=28)

The summary of the primary objectives for the implementation of the information security systems in the responding organizations is presented in Table 2. As expected, the confidentiality was reported to be the key objective for the information systems security since the data and information are the vital sources and power weapons for any organization to make proper business decisions for surviving and/or gaining competitive advantage.

Security Objective	Low Value	Median Value	Average Value	High Value
Confidentiality	2	5	4.6	5
Integrity	0	5	4.4	5
Availability	3	5	4.3	5
Authentication	0	4	4	5
Authorization	0	4	3.9	5
Accountability	1	4	4.1	5
Privacy	2	5	4.5	5

Table 3 Security Objectives (1 – Not Important; 5 – Very Important)

The privacy and integrity were selected as the next two important objectives for the information security system. This rating reflects the current legal requirements imposed by the federal and state governments to restrict the organization regarding the collection and usage of an individual data and information. The availability, accountability, and authentication were also relatively rated high by the responders. These three objectives are the essential and success factors for individuals and organizations using the Internet and other networks to properly and legally conduct their daily business.

The majority of the responders (twenty four out of thirty two) stated that the data and information were the primary organizational resources to be protected by the security systems as presented in Table 4. The physical assets were ranked the least important information resources for protection by the security

system. This is not surprising since the intangible damage of unsecured data, information, and processing functions can not be easily replaced or repaired as the other physical assets. The damage data, information and processing systems have the invisible power to ruin an organization's existence or survival.

Resource Type	Number Reporting	Percentage
Physical Assets	6	0.21
Processing Functions	9	0.32
Data/Information	24	0.86
All	5	0.18

Table 4 Resources to be Protected

The responders were asked to identify the likelihood occurrences of the different threats using a scale of 1 to 5 where 1 is unlikely and 5 is the most likely. Table 5 presents the summarized statistical values in terms of median and average. It was some what surprising to learn that inadvertent/accidental and technical failures are the top two threats encountered by the responders. This implies that the current security systems lack to include some routine training for preventing unintentional mistakes in handling and processing information system resources by the employee within the organization. In addition, the current security system does not have adequate technical equipment configurations to provide the organization with a flawless routine operation.

Threat Type	Median Value	Average Value
Inadvertent/Accidental	4	3.5
Deliberate	3	3.1
Mother Nature	3	3.2
Technical Failure	3	3.3
Management Failure	3	3

Table 5 Threat Sources (1 – Unlikely; 5 – Most Likely)

Organizations that used the information systems security were asked to ascertain the consequences generated by the threats in their institutes. Table 6 summarizes the percentage of each threat consequence in term of three categories that include possible occurrence, actual happening, and not applicable. It is interesting to note that the actual happening of the threats are less likely to strike the organizations compares with the expected or possible occurrence of the threats by the organization in most cases. This reflects that the responders do recognize the malicious consequences of the threats toward their organization assets. Therefore, the responding organizations have done a good job in implementing some security systems to protect their information resources and prevent the actual occurrence of threats. The percentages in the not applicable category are due to diverse business practices of the responding organizations that will produce dissimilar threat consequences.

Responders were asked to indicate their implemented threat incident identification mechanisms when their organization encountered any security threat. Table 7 presents the statistical average value for each detection method corresponding with the number of reporting organizations. The detection devices and monitoring tools are the most widely used methods to report the security threat incidents. This is not surprising since these two approaches are either software or

hardware. They can monitor and detect the security violation automatically after their installation without any human intervention.

Threat Consequence	Possible	Actual	Not Applicable
Corrupted Operations	0.46	0.21	0.32
Comprised Systems	0.43	0.21	0.36
Loss of Service	0.32	0.43	0.25
Loss of Assets/Resources	0.50	0.11	0.39
Loss of Data Integrity	0.61	0.07	0.32
Loss of Information Privacy	0.68	0.11	0.21
Loss of Customer Trust	0.50	0.07	0.43
Loss of Customer	0.32	0.04	0.64
Loss of Sales	0.21	0.00	0.79
Loss of Profit	0.29	0.00	0.71

Table 6 Threat Consequences (Percentage Value with n=28)

The system down time and audit logs has the second highest usage score. They are semiautomatic methods with some human intervention. They are statistical reports generated by the software program of the hardware and require the security personnel to conduct the interpretation and take action. It is interesting to note that the internal incident reporting process has scored the third highest rank among the eleven incident identification mechanism. This suggests that the manual process such as policy or procedure is also an effective mean to identify the security invasions. It also implies that most of the responding organizations do implement a well defined reporting procedure for its employee to follow whenever he/she encounters a security problem related to a threat.

Identification Mechanism	Number Reporting	Average Value
Audit Logs	15	0.54
Detection Devices	22	0.79
Monitoring Tools	22	0.79
Internal Incident Reporting Process	13	0.46
External Incident Reporting Process	3	0.11
Advance Warning by Authorities	2	0.07
Advance Warning by Other Entities	6	0.21
Denial of Service	8	0.29
Data/Information Corruption	5	0.18
System Downtime	15	0.54
Termination of Communication	6	**0.25**

Table 7 Threat Incident Identification Mechanism (n=28)

Organizations that have come across security threats in their organization were requested to identify specific threat counter measures in terms of three different levels that have been deployed in their institution. Table 8 presents the summary results of the threat counter measures implemented in the administrative level by the responders. Sadly, more than half of the responding organizations did not conduct any security risk analysis or management control. In

addition, some responding organizations had not established any security police, security plan, disaster recovery plan, or operational plan in the administrative level even the security is an essential top down management issue for the entire institute in the current century.

Administrative Counter Measure	Number Reporting	Average Value
Security Policies	20	0.71
Security Plan	15	0.54
Risk Assessment	13	0.46
Disaster Recovery Plan	17	0.61
Operational Recovery Plan	16	0.57
Management Control	13	0.46

Table 8 Counter Measures: Administrative Level (n=28)

The summary results of the threat counter measures implemented in the technical level by the responding organizations are illustrated in Table 9. More than two third of the responding organizations have adopted technical counter measures to protect their information resources. This result reveals two facts about the current security hardware and software technologies. First, they can automatically monitor the information system and effectively block the undesirable intruders. Second, their implemental costs are affordable by most of the responding organizations regardless of the size.

Technical Counter measure	Number Reporting	Average Value
Firewall/Routers/Switches	26	0.93
Demilitarized Zone	20	0.71
Intrusion Detection System	22	0.79
Network Monitoring		

Table 9 Counter Measures: Technical Level (n=28)

The threat counter measures implemented in the operational level by the responding organizations are summarized in Table 10. It is interesting to note that twenty five out of the twenty eight responding organizations have well established the operational security procedures for personnel hiring and terminating processes. This appears that the employees are the most important security origin and foundation in the responding organization. It is understandable that a high percentage of the responders have some routine physical and procedure controls to protect their information resources.

Operational Counter Measures	Number Reporting	Average Value
Personnel	25	0.89
Physical	24	0.86
Procedure	24	0.86
Inventory	12	0.43
Monitoring	21	0.75

Table 10 Counter Measures: Operational Level (n=28)

As indicated, the inventory control is the least operational counter measures against the threats among the responders. This can be interpreted as the fundamental logistic process that separates the functions of purchasing and operating information resources to different department in the most responding organizations. Most likely, there is no centralized unit is charged with the responsibility to document the existence and change of the information resources.

CONCLUSION

The results of this research strongly suggest that (1) organizations today are implementing some security systems to protect their information resources; (2) the top management personnel such as chief executive officer does involve in the security decision making process; (3) the major objectives for the organizational security systems are information confidentiality and data privacy; (4) the most important resources to be protected are information and data in the organization; (5) the inadvertent/accidental incident is the most occurred threat; (6) loss of service is considered as the major consequence among all threats; (7) the automatic hardware and software tools are the most popular mechanisms to detect threats; and (8) the administrative controls are the least threat counter measures comparing with the technical and operational controls.

REFERENCES

1. Comer, D. and D. Stevens, Internetworking with TCP/IP, Prentice Hall, 2000.
2. Porter, M., "Strategy and the Internet," *Harvard Business Review*, March, 2001, 63-78.
3. Von Solms, V., "Information Security Management: The Second Generation," Computer and Security Vol. 15, 30-38, 1997.