ORGANIZATIONAL SECURITY DEVELOPMENT MODEL FOR E-BUSINESS

Nancy Tsai
School of Business Administration, California State University, tsain@csus.edu

Stephanie Berrington
California Public Employees' Retirement System (CalPERS), sdberrington@comcast.net

ABSTRACT

This research project centers on the information system security development issues for the business organization using the Internet to conduct e-business. The major objectives, threats, risks, and countermeasures of the information system security for the e-business gathered from the existing research literature will be summarized. A generalized development model for the e-business information system security infrastructure is proposed. Finally, the statistical results gathered from a national survey for the current security practices in the business organization will be presented.

KEYWORD: security, information system

INTRODUCTION

The advanced hardware and software technologies have interconnected numerous computers together to form an infinite and public information network named the Internet that can inexpensively transmit messages, voices, and images with the speed of light between the largest city and smallest town in every continent. The capability and characteristic of the Internet have succeeded in bringing disparate individuals to connect, communicate, and share information as a global community, regardless of the geographical distance and time difference.

The business organization has quickly realized and captured the Internet's benefits by expanding the traditional brick and mortar sales channel to a variety of newly developed e-business models that electronically offer information, services, and products to its customers and partners in order to improve the strategic values of the standard business process for more profit or less cost (Porter, 2001). In addition to its many positive advantages, the Internet has also brought a severe and different security problem to existing information systems for the business organization that utilizes the e-business as a communication and/or sales channel between its business partners and customers.

Information system security is always an essential issue for any business organization, from daily operations to its ultimate survival. Prior to the establishment of the Internet, most computer hardware, software, data, and information were centralized and physically secured in the locked computer room that was carefully managed by experienced data processing center staff. Any inter business communication was accomplished through the utilization of closed private network technology to guarantee information privacy and

confidentiality. The threats to the information system security were basically related to the behavior of the employee in the organization such as misusing the data, theft, vandalism, accident, software error, hardware failure, and natural disaster, etc. These threats were well understood and could be prevented or rescued through a set of standard backup and recovery techniques.

On the other hand, the business organization has had to replace its centralized computer system with the client/server architecture for the purpose of connecting its network to the Internet in order to facilitate the retrieval and distribution of information. However, the open and standard transmission control protocol and Internet protocol (TCP/IP) used in the Internet for delivering the data was developed without security considerations (Comer, 2000). Not only the identification of the sender and receiver addresses, but also the transmission data, can easily be intercepted, interpreted, and altered by an unauthorized information hacker if no other security measure is implemented to protect the transmission. In addition, the computer virus generated by an information terrorist can be transmitted through the Internet to significantly damage the information and paralyze the computer information system of a business organization.

The flexible and extensible Internet connections promote and expose the business organization's network to a new level of electronic risk. The traditional method of securing information system no longer meets the new requirement since the threat and warfare are a mouse click away by anyone with Internet access from anywhere in the universe. Therefore, it is essential to have a thorough and effective information system security with an adequate infrastructure and constant re-engineering for the business organization to counter the new security challenges generated in this current Internet information age.

This research project centers on information system security development issues for the business organization that uses the Internet to conduct any type of e-business. The major objectives, threats, risks, and countermeasures of information system security for the e-business gathered from the existing research literature will be summarized. A generalized development model for the e-business information system security is proposed. Finally, the statistical results gathered from a national survey for the current security practices in the business organization are presented.

THE INFORMATION SYSTEM SECURITY ISSUES

The e-business has opened an electronic universe that offers opportunities and threats for the organization conducting business. The organization needs to rethink its information system security strategy and develop a new security management approach to capitalize the benefits and minimize the risks at the same time (Von Solms, 1997). The fundamental security attributes and components can be identified as objective, asset, threat, risk, and countermeasure in analyzing and dealing with the overall information security plan of the organization.

The objectives for security provide a set of benchmarks that can be used as strategic criteria with which to measure the effectiveness of a security plan. Moreover, they can also serve as guidelines to identity the required countermeasures to protect the physical and logical assets from internal and external threats. Therefore, it is essential to clearly understand the real meaning of each individual objective before analyzing other components. The most common objectives can be described as availability, integrity, authentication, accountability, confidentiality, privacy, authorization, trust, and security.

The assets of the organizational information system include computer hardware, software, database, physical facility, and human resource. Computer hardware consists of the electronic devices to perform information system operations such as input, processing, storage, output, communication, networking, and security in a client/server environment with or without physical wires. The software is a group of computer programs to instruct, control, and coordinate computer hardware for generating and presenting the information. The system software, application software, and middleware are the three major types of software. Database is the central depositories for the interrelated data files that allow the organization to analyze the information for searching its competitive opportunity.

The physical facility is composed of buildings and other physical resources to provide a working environment for the entire organizational information system. Last, but not the least, are the human resource that includes a cross-functional team of different skilled staff members to develop and manage the information systems. They consist of the traditional employees with computer knowledge such as project manager, system analyst, programmer, network specialist, security personnel, database designer, and operator. In addition, the team is comprised of experts from additional areas such as marketing, sociology, psychology, law, and management, etc. to deal with new international business issues related to the e-business applications.

The threat to the information system interpreted as computer crimes in general includes (1) the unauthorized use, access, modification, and destruction of hardware, software, data, or other information resources; (2) the unauthorized collection, storage, and release of information; (3) the unauthorized copying and usage of software; (4) denying the end user information retrieval from the system; and (5) using the information system resources to illegally obtain information or tangible property. The specific new threats generated from the current e-business environment consist of viruses, spam emails, web page defacements, denial of service, cookie modifications, cross-site scripting, hyperlink parameter tampering, cyber theft crime, cyber terrorism, time theft, and resource theft.

The countermeasure is a set of control tools or methods to protect the entire organizational information system asset against the threat. There are three interrelated controls named physical, technical, and administrative. The physical control uses different door locks, human guards, and surveillance cameras to prevent the unauthorized access and avoid malicious vandalism and theft of the asset. This can also be achieved by more advanced biometric access controls that utilize a unique personal trait. In addition, the environmental code with proper temperature, humidification, smoke detector, and fire extinguishing methods, etc. are also included in this control.

The technical control utilizes the modern computer hardware and software technology to protect the organizational information system asset. This includes the authorization and authentication for the system access control, data encryption and decryption for the transmission confidentiality, digital signatures and electronic certificates for increasing trust and accountability, network monitoring programs for operation availability and security, and firewalls for protecting the organizational intra network from outsiders.

The administrative control establishes a management framework of security policies and procedures for the end user and system personnel to follow. It composes of (1) the management involvement issue for determining the security strategy and allocating annual budget; (2) the personnel management for hiring, terminating, and security training; (3) the resource usage standard for preventing improper conduct; (4) the access control guideline for wire and remote environments; (5) the contingency plan for recovering from any natural and manmade disaster attack; (6) the auditing guideline for the information resource and asset; (7) the documentation control for hardware and software inventory; and (8) the environment code for housing assets.

The risk is the negative impact on the organization due to the absence of security countermeasures for the information system assets and resources. The tangible damage can actually be measured in terms of dollar amount from the physical asset replacement. The intangible effect needs a rough estimation of the associated dollar value for the loss of sales, profits, customers, productivity, data integrity, individual privacy, customer trust, and reputation of the organization.

THE INFRASTRUCTURE DEVELOPMENT MODEL

The dynamic development model utilizes four different stages named plan, analysis, implementation, and re-engineering to create the security infrastructure for any organization. In the plan stage, a security committee is first formed with members from information security division, top level management, and the end user of every division. This committee defines the objectives, standards, guidelines, budgets, and constraints for the security infrastructure of the entire organization.

The tasks to be accomplished in the analysis stage consist of the following: (1) a list containing the asset, threat, and countermeasure for the critical information resources in terms of carrying out the routine business operations by the information staff member; (2) the risk associated with every threat for each asset by the end user; (3) estimating the dollar value of the countermeasure and the risk for each threat as accurately as possible; (4) determining a weighted factor to indicate the relative importance of the countermeasure for an asset; (5) assigning a threat occurring probability; (6) assessing the actual value of each countermeasure by the threat occurring probability; (7) calculating the security value by taking the difference between the total value of all risks and the total actual value of the countermeasures; and (8) finalizing the security implementation priority list using the security value and weighted factor.

The implementation stage is the construction of the security system according to the security implementation priority list that is defined in the analysis stage. It has two parallel assignments. The first assignment can be considered a logical oriented one in that it is the detailed description of the security procedure under the policy and guideline specified in the plan stage. It includes (1) the access and usage of each asset; (2) the hiring, terminating, and training of personnel; (3) the inventory of hardware and software; (4) incident management; (5) environmental issues; and (6) the auditing process. On the other hand, the second assignment is the physical implementation corresponding to the item listed in the first assignment.

The last stage is the re-engineering that is the vital point to support the building of a dynamic security infrastructure for the organization to meet the constant threat challenges imposed by the e-business. This stage continuously generates the security information by gathering the data from (1) incident reports; (2) auditing results; (3) new threats; and (4) the countermeasures for the current security information technologies. These internal and external security feedbacks become the input to the three previous stages. The security plan, analysis, and implementation stages are continuously updated and revised to counter any new threats to better safeguard the organizational information asset in the open environment of the Internet.

SURVEY RESULT

The statistical analysis from a national survey using US post office, email, and web site for the current security practices in the business organization will be included in here.

CONCLUSION

The proposed model has the following features (1) it suggests a top down security development approach; (2) it integrates the security strategy with the corporate level business strategy for the entire organization; (3) it supports the dynamic security infrastructure to incorporate the current information technology as an offensive or defensive tool for protecting the information asset; and (4) it adopts a flexible process to select and implement a set of the most effective counteractions within the available resources for achieving the organizational security objectives.

REFERENCES

1. Comer, D. and D. Stevens, *Internetworking with TCP/IP Principles, Protocols, and Architectures*, 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.