

PROTECTING INFORMATION SYSTEMS AND DATA OF COMPANIES

by
Valerie Barnes
Robert Campbell
Linda Kelly
Carey Land
Stephania Million
Dan Rohan

Prepared for

Dr. Fane

Accounting 4401

Accounting Information Systems

University of North Florida

April 15, 2002

Information systems are an integral component of doing business today. Individuals, companies, and governments rely on their information systems to function properly. A loss of data or a breach of security can be financially devastating. Monetary losses can be avoided, however, through proper protection of an organization's assets. To protect an information system and its data, the potential threats must be identified along with the internal controls used to guard the structure. Specifically, general controls can be used to safeguard data. The success of internal and general controls, however, depends upon having competent personnel with the necessary training and certification. With the proliferation of computer crimes, many certified individuals are specializing in the growing field of computer forensics. These specialists are able to retrieve evidence that was once thought to be unrecoverable. The U.S. Government is also establishing standards that will not only improve the protection of information systems and data for itself but for the private sector as well.

A company's information system and data are its most important assets. Companies fail to realize the value of their data and, therefore, do not protect the data properly. Companies need to enforce policies, procedures, and controls to ensure the protection of their information systems and data.

Information systems face four different types of threats. The first is natural and political disasters, for example, floods, fire, earthquakes, and war. The second type of threat is software errors and equipment malfunctions, which would include hardware failures, power outages, and undetected data transmission errors. Another threat is unintentional acts. These are the most common of all four threats and result from human errors. According to Carl Jackson, former president of the Information Systems

Security Association, unintentional acts account for around 65 percent of all security problems that companies face (Romney & Steinbart, 2000). The last threat is the least common and is referred to as intentional acts, which take the form of sabotage, computer fraud, or embezzlement.

Companies can implement controls to minimize the threats to their information systems. Controls not only minimize the actual threats, but they can also minimize the extent of the damage a threat can cause. Accountants need to know how to protect systems from threats because accountants play a significant role in helping a company implement these controls. If a threat does actually occur, an accountant must be able to detect, correct, and recover the system.

A company can use internal control as a basis or guideline to help protect its information system and data. Romney and Steinbart define internal control as “the plan of organization and the methods a business uses to safeguard assets, provide accurate and reliable information, promote and improve operational efficiency, and encourage adherence to managerial policies” (2000, p. 253).

Internal control has four classifications. The first classification is preventive, detective, and corrective. Preventive controls are implemented to keep the threat from ever occurring. If a threat does materialize, a company should have controls to detect the occurrence. Finally, corrective controls take care of problems found in detective controls. The next classification of internal control is general and application. General controls ensure the overall control environment is in good condition. Application controls help prevent, detect, and correct problems in transactions while being processed. The third classification of internal control is administrative and accounting,

which include operational efficiency and safeguarding assets. The final classification of internal control is referred to as input, processing, and output. These controls ensure the accuracy of data as they move through the system.

The protection of information systems and data has become so important to organizations that there have been studies to provide guidelines for evaluation of controls. Based on a three-year study, the Committee of Sponsoring Organizations (COSO) has designed an internal control model. The internal control model consists of five components, which are control environment, control activities, risk assessment, information and communication, and monitoring. The control environment is basically the foundation of the organization and its philosophy. Control activities, which are policies that ensure the company's objectives will be achieved, are imperative in keeping a company's data safe. Risk assessment involves the identification and analysis of risks to the information system. Information and communication support the other control components by communicating control responsibilities to employees and by providing information in a form and time frame that allows employees to carry out their duties. The final component of the internal control model is monitoring performance. Monitoring includes effective supervision, responsibility accounting, and internal auditing.

In December 1999, an article published by The Institute of Internal Auditors summarized COSO's model. According to the article, Boeing adopted the internal control model and reported that the COSO model provided the foundation for all its audit work. A company as large as Boeing needs some type of control framework. Boeing has reported several benefits resulting from COSO's internal control model such as

improved reporting on internal control status, efficiency of projects, and effectiveness of audit work. The company feels the reliability of its audit work, however, depends on continued adherence to the model. Boeing will implement peer reviews and ongoing monitoring to improve the reliability (Applegate & Wills, 1999).

For a company to adequately protect its data, it must use general controls to manage data transmission, logical access and data storage. A company must have the right tools and techniques to implement this type of control. Management must also understand how these tools work and their capabilities.

A company that has good data transmission control will use firewalls, tunneling, and encryption to safeguard information entering and leaving the system. There are many different types of firewalls. The packet-filtering firewall is the most common because of its simplicity and low cost. It controls “access to a network by analyzing the incoming and outgoing packets” (Strom, 2000, p. 1). These packets contain the identity of the source that is transmitting the information. The firewall is able to decode the data through its source address, source port, destination port, and connection status. One disadvantage of a packet-filtering firewall is it cannot detect viruses or bugs that are being sent through these connections. For this reason, most companies use firewalls as a first line of defense and not as a primary data control.

Some companies will also adopt a tunneling technique when using firewalls. Tunneling can be used within a company’s own network or to connect it to another company’s network. The two networks “are connected via internet- firewall to firewall- and data is divided into small segments called internet protocol packets, encrypted, mixed with millions of packets from thousands of other computers and then sent through

the internet” (Romney & Steinbert, 2000, p. 305). Each packet is decrypted and then formed to its original data. Tunneling creates a secure line that is difficult to translate by an outside source.

Encryption is another way a company can protect the transmission of data. Encryption can safeguard the confidentiality, integrity, and authenticity of data (Romney & Steinbart, 2000). Encryption transforms data into a different format using algorithm functions. When an encrypted message is received, the data can be translated back into the original format through codes. Encryption is very successful as long as the codes are kept safe between the sender and receiver.

Logical access controls are used to safeguard information within a system or network. The use of passwords, compatibility tests, and biometrics can limit who has access to a company’s data. Passwords are an effective tool in determining who has access to a particular system. They are easy to implement into a system and can be changed periodically. Passwords can become a hazard if the wrong people discover them. If an unauthorized person has the correct password, the system will grant access, and the violation of security will go undetected. Biometrics can be used to prevent this from occurring. “Biometrics are technologies that automatically authenticate, identify, or verify an individual based on physiological or behavioral characteristics. Examples include products that recognize faces, voices, and finger prints” (Dornbush, 2002, p. 1). Biometrics technology is one of the most secure ways to control access to data because it is almost impossible to copy unique characteristics.

Data storage controls are also important when keeping data secure. All data, which are stored internally on the hard drive of a computer or on diskettes, must be

properly labeled. If data are not labeled and stored properly, they become vulnerable to outside tampering. There are numerous ways to label data. A volume label, an external label, and a trailer label are all internal labels that can be used to identify the contents of a file, and they assist in organizing and determining where files go. A tape file protection ring protects data from being altered. Once the ring has been removed from a disk, the data within the file cannot be changed. These write protection mechanisms are a great way to secure records and other historical information that will not be changed.

Perhaps, the only way a company can know that its information assets are truly secure is to use competent personnel, whether it be through the direct hiring of personnel or contracting for security-related services with an outside firm. A company can buy all of the latest security technology in the world, but the secret to information systems security lies in the strength of the professionals in charge. According to James E. Duffy, managing director of International Information Systems Security Certifications Consortium, Inc. (ISC2), “as Internet security threats continue to rise, many organizations have unwisely focused on technology solutions alone in protecting information assets” (2001, p. 13).

Companies can have confidence in the abilities of their associates when they hold one of the certification designations for information systems security professionals. ISC2 is one of the organizations charged with training and testing individuals for professional certification in the data security industry. ISC2 is not-for-profit and offers two certification designations, Certified Information Systems Security Professional (CISSP) and System Security Certified Practitioner (SSCP). The CISSP designation is the most desirable, requiring the most experience and training.

When a company hires someone with the CISSP designation, it is investing in a person who has experience in the data security industry and has passed a rigorous comprehensive examination. CISSPs must adhere to a professional code of ethics and must stay current regarding the latest information security issues through continuing professional education. It costs between \$2700 and \$3200 per individual to be trained and tested for the CISSP designation (2002, p. 4). Companies and individuals who achieve this level of professionalism are serious about protecting information assets.

An extensive knowledge about information systems security is required to become a CISSP. Candidates for certification are currently required to have a total of three years' experience in one or more of the ten domains within the information security industry. The CISSP examination is a rigorous six-hour undertaking that covers all ten domains of the Common Body of Knowledge (CBK) established by ISC2. These domains are the following:

- (a) Security management practices
- (b) Security architecture and models
- (c) Access control systems and methodology
- (d) Application development security
- (e) Operations security
- (f) Physical security
- (g) Cryptography
- (h) Telecommunications, network, and Internet security
- (i) Business continuity planning
- (j) Law, investigations, and ethics (2002, p. 1)

Just as the information security industry is continually evolving to keep pace with ever-increasing security threats, so is the ISC2 professional designation process. The CBK and CISSP exam is continually updated with the most current information. More stringent requirements for the CISSP designation will be enacted as of January 1, 2003.

Candidates for the CISSP designation will be required to have a college degree as well as a cumulative three years' experience in one or more of the ten domains.

A company that hires certified personnel and conducts business with organizations that have passed rigorous information security training programs indicates to the public that information security is a top priority. By demonstrating a known level of competence regarding information security, companies can significantly lower risks associated with protecting data assets. Customers and investors will have confidence that their investments are being protected.

Companies are noticing the importance of public trust and the need for trained professionals to help protect the integrity of their information systems. ISC2 has certified more than 7,000 information systems security professionals in more than 60 countries. Estimates are that 60 percent of chief information security personnel will be required to hold a professional designation. ISC2 has certified professionals in such organizations as Ernst & Young, KPMG, NASA, and the Social Security Administration.

Additionally, Deloitte & Touche (D&T) has been added to the list of ISC2 clients. D&T recently completed a rigorous information security program in its Canadian offices. Over half of the D&T Secure e-Business practitioners were awarded the CISSP designation. "In today's e-business environment, companies need to be assured their information assets are being protected by the most qualified security professionals available," according to Adel Melek, D&T partner and Canadian national leader for Secure e-Business (2001, p. 13).

The proliferation of computer threats, both internal and external, has led many information systems security professionals to enter the growing field of computer forensics. Computer forensics "is the science of capturing, processing and investigating

data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law” (Vogon, 2002, p. 1). Lack of security can expose a company’s information system and assets to widespread loss. The use of computer forensics can prevent, detect, and correct weaknesses in a company’s system.

Computer forensics has the ability to search through stored data, whether it has been manipulated or deleted. Trained professionals can use software to find hidden files, uncover deleted files, indicate file modifications, monitor Internet activities, monitor file downloads, and retrieve portions of lost documents (Eagle, 2002). To be a computer forensics specialist requires a variety of skills. Moreover, one must have knowledge of different networks, programs, operating systems, monitoring software, and recovery tools and techniques. If a company suspects unlawful activity, it should hire a certified professional. A layman could inadvertently destroy the necessary evidence for prosecution.

Many cases illustrate the benefits of computer forensics. For example, Rehman Technology Services of Mount Dora, Florida, a computer forensics company, was involved in a case where employees were suspected of stealing information from their current company to gain knowledge to start their own business. A month or two before the workers were to leave, employers hired Rehman Technology Services to find out whom the employees had contacted, which clients they planned to steal, and what projects they wanted to duplicate (Pfister, 2002).

“Loek Weered, police inspector and expert for the computer crime unit of the Haaglanden regional police in the Netherlands, says that computer users, around the world, have made themselves targets for computer crime by being so dependent upon information and

communication technology” (Armstrong, 2000, p. 2). There is no crime scene in cyberspace, which gives criminals the advantage and makes it more appealing to commit an unlawful act. Since the criminal can access data on their own computer, “ethical limitations like what is yours and what is mine seem to disappear” (Armstrong, 2000, p.2).

The downfall to this growing crime is that laws to regulate control lag behind technological advancements. Still, when caught, these perpetrators rarely go to court due to the extensive evidence that can be presented in court, so most cases are settled out of court. Computer forensics can show proof of what employees have been up to, files that have recently been accessed, attempts to destroy evidence, Internet activity and more. Federal laws are in place to protect companies against these computer crimes. When computer forensics is used and evidence is retrieved, a company can prosecute an individual. Penalties for these crimes include up to 15 years in prison and/or restitution paid.

The potential for loss to companies is massive. Over the past few years, advances in technology have seen large growth spurts. However, the industry’s growing pains have consisted of a lack of security measures that have increased criminal activity. Experts believe that computers, in some form or another, will be involved in almost every crime in the near future. The growing usage of the Internet, e-commerce, and e-mail, supports this theory. For this reason, companies must protect their digital assets. A computer is often treated as if it were a calculator, when in reality it is a large filing cabinet holding the keys to a corporation (Armstrong, 2000).

Internally there are many ways for a company to prevent fraud. Using proper hiring and firing techniques, managing angry employees, training employees in security and fraud prevention measures, and segregating duties can reduce risk. With

advancements in technology, seemingly someone is always ahead of the game. Experts recommend having a computer forensic specialist available at all times to protect assets. In addition, every organization should have a structured incident response plan, which should include access to the appropriate management monitoring computer activity. If suspicions arise, a professional forensic specialist may be needed.

The Federal government owns one of the largest data management systems in the U.S. For reasons of national security, the protection of government data requires that systems be constantly monitored and upgraded to outsmart cyber terrorists. Prior to September 11, 2001, the National Security Council had already begun focusing on measures to protect the information systems and data security of the Federal government. However, the terrorist attacks created an increased urgency and necessity to securing America's most critical and sensitive information. While the events of September 11 were unfolding, Richard Clarke, national coordinator for infrastructure protection and counterterrorism, was speaking at the E-Gov Information Assurance conference in Washington, D.C. His speech focused on developing standards that would require a specific level of security in the commercial products bought by government agencies (Frank, 2001).

The protection of data and information systems is a continual challenge for the Defense Department. Even though standards for procuring secure operating systems exist, they are often ignored because so few commercial products have gone through the Department of Defense's Trusted Computer System Evaluation Criteria (Frank, 2001). However, these criteria will be replaced with an international standard called the Common Criteria Evaluation (CCE) developed by the National Institute of Standards

and Technology (NIST) and the National Security Agency (NSA). Civilian agencies are encouraged to adopt the new international standard, but the lack of availability of CCE-certified products will make application difficult (Jacobs, 2002).

According to Frank (2001), the Federal government is the largest single purchaser of computers and information technology. This gives the government tremendous influence over developers and vendors, and this power should promote the use of these more stringent requirements. The government will exert pressure through the enforcement of the National Information Acquisition Policy entitled National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 (Jacobs, 2002).

Over the past decade, the transition to a global market of varied and often conflicting interests has dramatically changed the way governments, companies, and organizations think about protecting their information systems and their most critical data. The following three factors dominate this new way of thinking:

- (a) The need for protection encompasses more than just confidentiality;
- (b) Commercial Off-the-Shelf (COTS) security and security-enabled Information Assurance (IA) products are readily available as alternatives to traditional NSA-developed and produced communications security equipment (i.e. Government-Off-the-Shelf (GOTS) products; and
- (c) An increased and continuing recognition that the need for IA transcends more than just the traditional national security applications of the past. (National Security Agency, 2000, p. 1)

Making it mandatory for COTS products to be assessed and confirmed under either the NIST Federal Information Processing Standards 140-2 or by using the International Common Criteria for Information Technology Security Evaluation is how NSTISSP No. 11 intends to strengthen security confidence (Jacobs, 2002).

The U.S. Government is stepping up to the plate to make this all happen. Through collaboration between the NIST and NSA, the National Information Assurance Partnership's (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) Program was developed. NIAP produces protection profiles and security targets, two very important document priorities of the CCEVS (Jacobs, 2002).

A protection profile is the user document which specifies the functional requirements needed or preferred by that user from a commercial IA or IA-enabled product. It also delineates the assurance levels the user wants from product testing. These profiles serve two functions. First, they create a forum for the user to specify requirements and to classify them by their priority to the user. Secondly, they match vendors with users based on the stated requirements thereby creating a ready market for the vendor's products (Jacobs, 2002).

Vendors are required to provide a security target document, which describes the security features of its product. The development of a security document is necessary to have a vendor's product evaluated (Jacobs, 2002).

Based on internationally certified methodologies and standards for testing, the NIAP Program manages the evaluation of commercial products. The benefit of this approach is that commercial vendors can have their products tested in many countries around the world and are not restricted to testing within their own countries. Any accredited commercial testing laboratory compliant with the Common Criteria Mutual Recognition Arrangement can administer the evaluations. This process assures consistency of testing quality around the globe. In addition to the U.S., there are 14 other countries currently participating in the NIAP Program (Jacobs, 2002).

In terms of the U.S. Government's total Information Assurance strategic plan, NSITISSP No. 11 is a vital policy component. Effective July 1, 2002, full compliance will be enforced. This is an important step in worldwide data and information system security because many security products available in the market have not been certified. With the new policy, many more should come into compliance and provide a larger pool of security technology solutions. Because of the current disparity between products, it is essential that new means be devised to validate performance and to assure these products meet the needs and expectations of the intended users (Jacobs, 2002).

Hopefully, the implementation of government standards will have a positive effect on the availability of reliable security products for the private sector and lead to a reduction of computer fraud. Dependable security products will not eliminate the need for information systems security professionals, however. The need for competent professionals, especially ones trained in computer forensics, will still be an important factor to maintain and guard the data and information systems of companies. Effective internal controls are ultimately the basis for a well-managed information system, and they should be a primary goal for management.

Reference List

Applegate, D. & Wills, T. Struggling to incorporate the COSO recommendations into your audit process? http://www.coso.org/Articles/audit_shop.htm, 12/99.

Armstrong, I. Computer forensics. http://www.scmagazine.com/scmagazine/2000_04/cover/cover.html, 04/00.

Dornbush, R. Biometric technology. http://www.biometrics.com/tech_dornbush.htm, 10/04/02.

Duffy, J.E. (ISC)² Press release. (ISC)² certifies Deloitte & Touche information security personnel. <http://www.isc2.org/cgi-bin/content.cgi?page=13>, 04/10/01.

Eagle Investigative Services. What is data forensics? <http://www.eaglepiservices.com/DataForens.htm>, 07/04/02.

Frank, D. NSC seeking security standard. <http://www.fcw.com/fcw/articals/2001/0910/web-NSC-09-12-01>, 12/09/01.

(ISC)². CISSP CBK review courses. <http://www.isc2.org/cgi-bin/content.cgi?category=15>, 08/04/02.

(ISC)². Common body of knowledge. <http://www.isc2.org/cgi/content.cgi?category=8>, 08/04/02.

Jacobs, M.J. Information assurance leadership for the nation. <http://www.NSA.gov/isso/2002021memo.pdf>, 15/02/02.

Melek, A. (ISC)² Press release. (ISC)² certifies Deloitte & Touche information security personnel. <http://www.isc2.org/cgi-bin/content.cgi?page=13>, 04/10/01.

National Security Agency. NSTISSP No. 11. http://niap.nist.gov/naip/library/nstissp_11.pdf, 01/00.

Pfister, N. Computer detective foils company theft. <http://orlando.bizjournals.com/orlando/stories/1999/09/13/smallb1.html>, 07/04/02.

Romney, M.B. and Steinbart, P.J. Accounting Information Systems (8th Edition). New Jersey: Prentice Hall, 2000.

Strom, D. The packet filter: a basic network security tool.

http://rr.sans.org/firewall/packet_filter.php. 25/09/00.

Vogon. About forensic computing.

http://www.vogon-computer-evidence.com/forensic_services-01.htm, 07/04/02.

APPENDIX A

Abbreviation List

CBK	Common Body of Knowledge
CCE	Common Criteria Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CISSP	Certified Information Systems Security
COSO	Committee of Sponsoring Organizations
COTS	Commercial Off-the-Shelf
D&T	Deloitte & Touche
GOTS	Government-Off-the-Shelf
IA	Information Assurance
ISC2	International Information Systems Security Certifications Consortium, Inc.
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSP Policy	National Security Telecommunications and Information Systems Security
SSCP	System Security Certified Practitioner

Annotated Bibliography

Applegate, D. & Wills, T. Struggling to incorporate the COSO recommendations into your audit process? http://www.coso.org/Articles/audit_shop.htm, 12/99.

This article summarized C.O.S.O.'s internal control model. The article emphasized how adopting the model can help a company in its auditing procedures. The article also explained how Boeing adopted the C.O.S.O. model and how effective it was.

Armstrong, I. Computer forensics. http://www.scmagazine.com/scmagazine/2000_04/cover/cover.html, 04/00.

This is an article from Security Magazine written in April 2002. It describes the profession of computer forensics. It covers the topics of forensic tools, crimes in other countries, issues of the court system, and the future of computer crime.

Dornbush, R. Biometric technology. <http://www.biometrics.com/tech/dornbush.htm>, 10/04/02.

A biometrics company wrote this article. It defines biometrics and provides information on how biometrics can be used to safeguard data. The article also goes in depth about the future of biometrics.

Eagle Investigative Services. What is data forensics? <http://www.eaglepiservices.com/DataForens.htm>, 07/04/02.

Eagle Investigative Services is an international firm dealing in computer forensics. Their website addresses the expectations one can have from hiring them to investigate computer crimes. They provide analysis of computers and data in criminal activities, onsite seizure of computer data in criminal investigations, analysis of company computers to determine employee activity, and many other services.

Frank, D. NSC seeking security standard. <http://www.fcw.com/fcw/articals/2001/0910/web-NSC-09-12-01>, 12/09/01.

This article addresses how government is attempting to improve IT products purchased by the federal agencies. Being required to meet a new standard, commercial vendors are trying to meet the demand but first must meet new "Common Criteria" certification. Old criteria seem to have been ignored, jeopardizing the nations information and data security.

Hummel, R. How it works: personal firewalls. <http://www.pcworld.com/hereshow/article.asp?aid=17012>, 05/06/00.

This article is about firewalls. It was written for the Pcworld.com website. An explanation of the benefits of using a firewall is discussed.

(ISC)². <http://www.isc2.org/>, 04/08/02.

(ISC)² stands for International Information Systems Security Certifications Consortium, Inc. The web site is a comprehensive look at the organization and the services it provides. It is organized into four main parts: information, training, certification, and post-certification. Each main section is subdivided further, providing a wealth of information regarding the certification designations available to information systems security professionals. Several sections of the web site are cited specifically throughout the paper.

Jacobs, M.J. Information assurance leadership for the nation.
<http://www.NSA.gov/isso/2002021memo.pdf>, 15/02/02.

In an attempt to address concerns of IT industry leaders, Mr. Jacobs created this directorate to answer questions regarding the importance of compliance to NSTISSP No. 11. What the policy is and why it is important to national security is explained.

National Security Agency. NSTISSP No. 11.
http://niap.nist.gov/naip/library/nstissp_11.pdf,
01/00.

This is the explicit fact sheet of NSTISSP No. 11. It describes the policy and directs the heads of U.S. governmental departments and agencies to comply by July of 2002 when purchasing any system used in relation to national security information.

Pfister, N. Computer detective foils company theft.
<http://orlando.bizjournals.com/orlando/stories/1999/09/13/smallb1.html>, 07/04/02.

This is an article from the Orlando Business Journal written on September 13, 1999. It discusses the importance of computer forensics relating to businesses. It highlights the company Rehman Technology Services, Inc. and the cases that they have investigated.

Romney, M.B. and Steinbart, P.J. Accounting Information Systems (8th Edition), 2000.

The textbook details the foundation of threats and control issues facing companies today. The book named Carl Jackson as the source for estimating the percentage of

threats to companies. The text also provided extensive information on the C.O.S.O. internal control model as well as methods a company can use to safeguard its data.

Strom, D. The packet filter: a basic network security tool.
http://rr.sans.org/firewall/packet_filter.php. 25/09/00.

This article was written for The Sans Institute. It discusses firewalls and how they can be used to protect the data of a company. It also goes into detail about how packet filter firewalls work.

Vogon. About forensic computing.
http://www.vogon-computer-evidence.com/forensic_services-01.htm, 07/04/02.

Vogon International is a forensic computer company. They develop hardware and software to meet forensic technology needs. The website addressed their services of evidence collection, forensic analysis, and expert witness.