Security Basics: A Whitepaper

Todd Feinman, David Goldman, Ricky Wong and Neil Cooper
PricewaterhouseCoopers LLP
Resource Protection Services

Introduction

This paper will provide the reader with an overview of information technology (IT) security and how to evaluate IT security issues. It is written for individuals who want a broad, high-level discussion of IT security issues. It is not within the scope of this paper to detail every security exposure or control.

IT security is a broad concept whose features will be covered throughout this paper. Breach of IT security can result in unauthorized access of resources, intrusion of viruses, theft of data, or destruction of technology infrastructure. Media exposure leads the public to believe that most security violations are the results of hackers or "outsiders", however many unauthorized acts including malicious acts are carried out by disgruntled employees or "insiders". This illustrates the importance of securing computer-based resources from both "outsiders" and "insiders". The recently released InformationWeek Security Survey, conducted by PricewaterhouseCoopers LLP, details some of the steps organizations are taking to protect themselves and their information. This survey may be accessed online at: www.informationweek.com\698\98iursk.htm

Who is affected?

Not long ago only large corporations and companies needed to concern themselves with IT security issues. Their effort to keep information proprietary was the main focus of the field. This is no longer the case. Technology has become so prevalent that it affects almost every aspect of daily life. Computers are at the core of most businesses, ranging from trading systems used on the stock exchanges to the sports web page that delivers last night's scores. Computers are responsible for maintaining bank accounts, medical records, Department of Motor Vehicles reports, and credit history. Clearly, everyone who has a credit card or uses an Automated Teller Machine (ATM) must be concerned with the accuracy and privacy of their personal information and therefore must be concerned with IT security.

Why is there concern?

Many factors have caused an increased awareness of IT security-related issues. Personal computers (PCs) are no longer used exclusively at the office. Home and recreational PC use has increased dramatically. Home PC owners are opting for Internet access which allows them to access resources such as the World Wide Web, newsgroups, and E-mail. Home users and businesses are also finding online shopping, or e-commerce, appealing because of the convenience, simplicity, and robustness. This widespread availability and acceptance of computers has dramatically increased the number of people with the ability to compromise data.

As prices continue to drop, and people become more comfortable with technology, the reliance on computer-based resources will continue to increase. As this dependence develops, security exposures may lead to disastrous results with possible financial and legal ramifications. At a minimum, a security breach will result in lost time and decreased productivity while a “clean up” effort occurs. More than likely however, the results will be much worse. Financial losses as well as non-monetary effects will occur. For example, if a law firm had confidentiality breached and client information was stolen, they would lose credibility and no longer be able to attract clients. They might also suffer legal liability such as fines and suspension from the bar association.

There is also much concern because of the overabundance of security postings in mailing lists, newsgroups, and web pages dedicated to security bulletins. The widespread announcements give many security administrators cause for concern because of the multiple postings and vast array of sources. Interspersed throughout the postings are hoaxes, or security warnings, that are not proven to be valid threats to a system. Determining what are good sources for security information is difficult and filtering out the false warnings will take time and require investigation.

Security Objectives

There are three main aspects of effective IT security: Confidentiality, Integrity, and Availability. These concepts are further discussed throughout this paper.

Confidentiality
Confidentiality is the concept that information is unavailable to those who are unauthorized to access it. Strict controls must be implemented to ensure that only those persons who need access to certain information have that access. In some situations, such as those with confidential and secret information, people should only have access to that data which is necessary to perform their job function. Many computer crimes involve compromising confidentiality and stealing information. The concept of allowing access to information or resources only to those who need it is called *access control*.

The most common form of access control is the use of passwords; and the most common form of security breach is the compromising of these passwords. Requiring strong passwords, smart cards or single-use-password devices (tokens) is the first step in preventing unauthorized individuals from accessing sensitive information and is the first layer of defense in access control. Protecting these passwords is one of the most fundamental principles of IT security.

Imagine your business as a typical suburban house. A system password can be likened to a front door key. No one can enter the house without the key, but it can easily be lost, misplaced, or stolen. Implementing a strong password policy is inexpensive, does not require technical skills and should be taken extremely seriously. Businesses should create and implement an IT

security policy that educates employees on good password selection, use duration, and confidentiality.

Another aspect of access control is the limitation of resources available to an employee once they have been authenticated in the corporate network. For example, the entire human resources department might need access to employee information such as addresses and birthdays, but only certain individuals within the department need access to compensation information. Perhaps you want to allow specific individuals to view, but not modify certain information. This very specific, or granular, access control is another layer protecting computer-based resources. Access control can be paralleled in our model house as well. The maid has a front door key so she can come in and clean, but that key does not unlock the door to your home office. Furthermore, the maid does not know the combination to the safe in the bedroom that contains your important documents.

Integrity

Integrity ensures that information cannot be modified in unexpected ways. Loss of integrity could result from human error, intentional tampering, or even catastrophic events. The consequences of using inaccurate information can be disastrous. If improperly modified, data can become useless, or worse, dangerous. Efforts must be made to ensure the accuracy and soundness of data at all times.

When the validity of information is critical, it is often helpful to design controls and checks to ensure accuracy. It may be important to ensure that information is useless if it is stolen. Encryption is the process that transforms information into some secret form to prevent unauthorized individuals from using the data should they acquire it. This prevents interlopers from reading or modifying the information.

A well balanced IT security policy will have complimentary proactive and reactive components. The proactive facet involves utilization of strong security controls, while the reactive approach includes auditing and monitoring those controls. In this complimentary approach, the proactive component may be a properly configured system that records all system access in a log. The network administrator performs the reactive component by reviewing those logs for suspicious activity and investigating any deviations from the norm. It is necessary to take both approaches in order to maintain effective security control. Suppose that every time a door in our house opened, the time of the entrance and the name of the person entering the room was recorded in a log book. Then, anytime something was missing from a room, you could consult the book and see who was in that specific room and question them.

Availability

Availability prevents resources from being deleted or becoming inaccessible. This applies not only to information, but also to networked machines and other aspects of the technology infrastructure. The inability to access those

required resources is called a “denial of service.” Intentional attacks against computer systems often aim to disable access to data, occasionally the aim appears to be the theft of data. These attacks are launched for a variety of reasons including both political and economic motivations. In some cases, electronic mail accounts are flooded with unsolicited messages, known as spam mail, to protest or further a cause. Additionally, these attacks could be an integral part of a coordinated effort such as bringing down a home banking system.

Ensuring the physical security of a network or system is one way to cover availability. By limiting physical access to critical machines or data sources, the incidence of inaccessibility will be reduced. If contact with these resources is restricted, accidents as well as occurrences of internal mischief will also fall. Similarly, protecting the network electronically is important if many entry points exist, especially from a public domain like the Internet. For example, a firewall is a computer that resides between an internal network, or intranet, and an external network, such as the Internet. The firewall regulates and restricts what types of data can flow between the two networks.
Imagine that at the base of the driveway to your house there is a gate with a security guard. This guard acts as a firewall, limiting those who can enter the grounds. So, if your child lost his or her key, the intruder who finds it could not then unlock your front door because the guard would stop them from approaching.

Another aspect of availability ensures that needed resources are usable when and where they are needed. Providing system redundancy, in the form of backup data, machines, and power sources will often ensure availability. Offsite storage of critical data will allow recovery if location security is breached. Additionally, backup servers will allow normal workflow to continue if primary network security is breached. While these forms of security will ensure availability, it is important to protect them from intruders and maintain confidentiality of their data. Referring to our example, suppose that we keep copies our important documents (i.e. birth certificate, last will and testament, stock certificates, deed to your house, etc.) in a vault at the bank. In the event of flood, hurricane, or other disaster, we still have access to these papers.

You must evaluate and formulate a security strategy focusing on these three objectives. Depending on your business needs, various levels of emphasis should be placed on each objective. For example, security policies of a national defense system will place the greatest emphasis on confidentiality, as classified and strategic information must be protected. A funds transfer system at a bank has a greater need for integrity, as monetary accounts must be accurate. Lastly, an emergency medical system will emphasize availability, as information and resources must be accessible at all times and in many locations.

Factors to consider

When developing a security policy, care must be taken to identify and understand relevant and valid security issues. Often resources can be wasted reacting to a high-profile hoax while a serious issue goes unnoticed.

When evaluating the effectiveness of a particular security policy, the resources being protected must be analyzed. The information stored in today's computers ranges from public domain material such as telephone numbers to highly sensitive data such as an individual's genetic makeup. It is not practical, nor is it possible to firmly secure all this information. The goal is to protect information in line with its relative value and importance to the business process.

A well prepared IT security policy should focus on allowing employees to access only the resources he or she needs to perform their job function. Those who need to see information should be allowed, and only individuals who need to modify information should be allowed. Controlling who has read access, ensures that information such as employee compensation remains confidential. Controlling who gets write access ensures that loss of integrity does not occur as a result of modified information. If employee bonuses were based on compensation, then modifying compensation information would result in incorrect bonuses being paid.

The first important consideration when designing a security policy is the sensitivity level of the data you are protecting. For example, a database with publicly available telephone numbers would not warrant any sophisticated security controls. It might be impractical to use extremely expensive hardware encryption devices to protect employee birthdays and home addresses since the amount of money or public reputation lost after this information is compromised, may not be greater than the cost of implementing the security protecting it.

Second, the relative costs, not only in monetary terms, should be considered. While the cost of the solution, in dollars, must be considered, the time and effort needed to secure a business must also be factored. If implementing security hinders business operations to the level that employees cannot perform their job duties, then security needs to be rethought. Also, if the data compromised is made public, the negative publicity and loss of business that is created toward your firm must be calculated.

Although many security issues exist, a number of them are not valid. It is difficult to determine which are real, and which are used to distract you from true security holes. For example, you might think you are installing a system level patch, when in reality, you are installing a Trojan horse that captures passwords. An area where hoaxes are prevalent is virus warnings. Often, security administrators spend more time discerning what are hoaxes, than on the real issues. Hoaxes are time consuming and costly to deal with. Validated warnings that are sent from the incident response teams have genuine return addresses and are usually digitally signed with the organization's key. You should never install a patch or file from an unknown source, and when installing validated patches, always try them in a test environment first.

Conclusion

As individuals and businesses increase information sharing, and communication via the Internet, vulnerability to attack or intrusion rises. Authorization, access controls, and confidentiality requirements are some examples of the technological components available in a multi-layered IT security policy. Other important components include education on password secrecy, a corporate security policy, and physical system security. The more educated security administrators and users are, the less likely hoaxes will be treated as true threats, and the more likely these people will be able to evaluate and create a tight security policy. In the world of technological evolution, everyone is a target of electronic crime and needs to be concerned about security.