Computer Crime, Vulnerabilities of Information Systems, and Managing Risks of Technology Vulnerabilities

With the popularization of the Internet, interest in computer crime, ethics, and privacy has gained momentum. News items describe identity theft, credit cards numbers posted on chat rooms, and child pornography web sites. For example, in July, 2001, MSNBC.com reporter Bob Sullivan reported that key personal data including Social Security numbers, date of birth, driver's license numbers, and credit card information was posted up in a chat room. Investigations have yet to reveal the extent or perpetrators. However, affected individuals have already experienced fraudulent financial transactions on personal accounts The rich and famous are not exempt from such experiences. Bill Gates, Steven Speilberg, and Oprah Winfrey are among the notables who have experienced identity theft. The Contributing Editor of TechTV, Jim Louderback, wrote a revealing article published in USA Weekend, August 10-12, 2001, describing his own ordeal of identity theft.

Information systems vulnerabilities cover more territory than just personal losses. Computer information systems are vulnerable to physical attacks, electronic hacking, and natural disasters. With computer information systems serving as the vital life blood of many organizations, managers must be aware of the both the risks and the opportunities to minimize the risks to information systems.

Discussion is divided into types of computer crime, information systems and technology vulnerabilities, and ways to manage the risks.

Types of Computer Crime

Typically, computer crime can be categorized by the type of activity which occurs. Four basic categories are utilized in describing computer crime. These are: theft, fraud, copyright infringement, and attacks.

Theft. Theft in computer crime may refer to either unauthorized removal of physical items such as hardware or unauthorized removal or copying of data or information. It is well known that laptop computers are targeted at airports and restaurants. The prize garnered with theft of a laptop is usually the data or information such as passwords for corporate systems contained on the laptops rather than the hardware.

Fraud. Fraud on the Internet may run the gamut from credit card offers which are utilized only to capture personal information, to investor postings which promote a stock or investment offer to encourage investment which will benefit the person posting the information, to medical and pharmaceutical -related sites which purport to provide correct medical advice or sell altered medications.

Copyright infringement. The Internet has provided a unique opportunity and environment for copyright infringement. This type of computer crime encompasses use of software, music, etc which is not appropriately acquired (purchased). Software piracy occurs more easily with the ability to post files for downloading all over the world. However, another more costly copyright infringement occurs when trademarks and logos of corporations are posted on non-authorized web sites. Some criminals utilize the trademarks and logos to appear to be a legitimate site to perpetrate fraud. Many corporations have employees or consulting contractors who constantly crawl the web to sniff out illegal usage of trademarks and logos.

Attacks on organizations and individuals. Attacks on organizational information systems may be either physical or logical. There are several instances of web sites, products, and individuals being libeled or attacked by individuals or groups. One of the classic examples was the attack on Proctor and Gamble as an occult organization. AOL and other ISPs cooperate fully with criminal justice systems to reveal identities of those deploying web sites of question.

Denial of Service Attacks (DoS) target specific web sites and associated servers. Some of the newsworthy examples of DoS during 2000 - 2001 have occurred at Microsoft.com, eBay.com, and Amazon.com. Web servers and connections can only handle so much traffic so Denial of Service (DoS) usually take the form of one of two ways:

- Coordinated attack (typically from unsuspecting desktops) to a particular IP address or URL requesting a page – overwhelms server and DoS occurs
- Attack sends incomplete packets so that traffic gets jammed with requests for re-send.

Information Systems and Technology Vulnerabilities

There are several classes of activities which may also harm information systems and supporting technology. These activities may result in criminal charges depending upon the circumstances and impact on information systems. Currently, these activities fall within classes of viruses, worms, Trojan Horse, time bomb, logic bomb, and trapdoors.

Viruses. A virus is a program with intent to harm or render a computer system useless. The virus method of attack is to attach itself to specific files such as data files. It is not a free standing program. It copies itself when the infected file is executed.

A virus can damage data, delete files, erase your hard drive, or just cause annoying screen displays or sounds. Viruses may hide within macros of Word or Excel documents. Some viruses are programmed to trigger execution on a particular date or time. Viruses do not cause hardware damage. Viruses spread from file to file. There are thousands of documented viruses!!!! Some recent examples of viruses include the Melissa, Chernobyl, and Michelangelo.

Most virus protection software provides monthly updates to ensure that the computer system is covered from recent virus discoveries. Two of the more popular versions of virus protection include Norton (Symantec) and McAfee.

Worms. Worms are another destructive program designed to create instability information systems and supporting technology. Worms differ from viruses in that a worm is a free standing program. A worm executes on its own functionality. Worms spread from computer system to computer system rather than from file to file.

Examples of notorious worms include the July and August, 2001 attack of CODE RED on IIS servers. IIS (Internet Information Services) is part of the Microsoft Windows Server operating system which provides internet connectivity. Servers including federal government web sites, Qwest DSL servers, and other corporate or governmental sites were hit.

A worm can reply to e-mails while attaching itself to the e-mail; can destroy File Allocation System (FAT) on Windows systems and other similar attacks on other files systems on hard drives. Because worms are free standing, they can spread on their own and do not require human intervention to spread. Thus, in some ways, worms are more lethal than viruses.

Trojan Horse. This software derives its name from the Greek mythology depicting war activity

between the Greeks and Trojans of Troy. The Greeks pretended to depart the besieged Troy but left behind a giant wooden horse as a "gift". The Trojans brought the horse within the gates of Troy and Greek warriors were hidden in the horse. The Greek warriors then captured Troy. Therefore, the Trojan Horse appears to have one function but in reality does something else.

Typically, a Trojan Horse performs something destructive while the person at the keyboard thinks they are downloading an animation or some other file. The Trojan Horse commonly either loads a software program to be utilized in a later Denial of Service attack or reads your passwords, credit card numbers, etc., saved within your system. This vital information is later used to make purchases or other criminal activities.

In August of 2001, a particularly damaging Trojan Horse named the Trojan Offensive has been reported. It damages the Registry of Windows operating system so that the system is trashed. (More on the Registry under Operating Systems.)

Time bomb. These are software attacks that are designed to occur at a predetermined time or date. The difference between a time bomb and a virus such as the Michelangelo is that technically the time bomb does not spread. It impacts on the system upon which it has been loaded.

Logic bomb. Logic bombs are software attacks that triggered by a predetermined event. The most common logic bombs occur when information technology employees are laid off from employment. Then, for example, billing systems go awry when an employee id number is no longer on the payroll database.

Trapdoor. Trapdoors are system entrances that circumvents security system. These are hidden logins or administrative user definitions added by system developers for unscrupulous reasons. Trapdoors allow an unauthorized or unknown user to control a computer system. Trapdoors are typically only aimed at servers or mainframe corporate systems.

Ways to Manage the Risks Associated with Vulnerabilities

As businesses and individual depend more and more on computers for storage of data and production of information, the capability to conduct business is vulnerable to attacks on computer systems. In addition to malicious attacks, there are always accidents and careless behaviors. Are backups really current? What happens if a pipe breaks causing flooding? These are examples of careless behaviors and accidents. There are electrical storms, fires, tornadoes, hurricanes, earthquakes, and other nature related events for which information systems must be prepared.

Managing the risk of computer crime. Protecting systems and data with passwords, encryption, auditing software, and access logs is vital. These logical protections must be reviewed and analyzed in order to ensure the system has not been penetrated.

Physical entry to computer systems must be protected. Locations of computer systems are often times hidden from the public knowledge in order to make the systems more difficult to find. Card key systems and login/logout of entry and exit to computer systems should be a regular business procedure.

Managing the risk of fraud. Regulatory agencies and criminal justice units are using the web to locate fraud. Regulatory agencies such as the FDA review medical and pharmaceutical related sites. Also, professional organizations such as the AMA and credible health care organizations

such as Mayo Clinic provide correct information on sponsored sites.

Managing the risk of copyright infringement. Businesses are learning to crawl the web for attacks and copyright infringements. Disney and Coca Cola are particularly vigilant. Bloomberg Financial was the victim of a spoof site which created quite a stir in the financial community.

Managing the risk of technology vulnerabilities. The major activity deployed by businesses to protect computer systems and data from electronic intrusion is the utilization of firewalls and virus protection software.

Firewalls are utilized to establish a barrier between the business computer systems and the outside world. Firewalls may be a combination of hardware and software or it may be software only. A firewall filters or restricts access externally to enter system and access internally to exist system. The usual implementation of a firewall is to place a barrier between a computer system and the Internet. There are four basic actions firewall software can take when communication is attempted. These are:

Piece of information can be dropped

- Alert issued
- Returned to sender
- Log action & receipt of information.

Communications are classified as inbound and outbound. When an attempt is made from another system to connect to your system, this is considered an inbound connection. And, when your system is attempting to connect outside of local, this is considered to be an outbound connection. Once the connection is allowed, bi-directional communications can occur without filtering. Therefore, firewalls must be set too restrict access both inbound and outbound.

Virus protection software must be kept current as new viruses are developed on what seems like a daily basis. Some businesses have policies that limit acceptance of attachments to e-mails, prohibit the use of disks prepared on non-business systems, and restrict downloading files from the Internet from trusted sites only.

Special considerations for home and small businesses

Individuals and small businesses are employing faster ramps to the Internet with cable modems and DSL (Digital Subscriber Lines). These connections are always "On" when your system is on regardless of whether or not you are actually on the Internet via a browser. System is vulnerable to attack. Therefore, such subscribers should deploy a firewall to protect systems connected via cable modem or DSL. Norton (Symantec) Personal Firewall and Black Ice Defender are two firewalls designed for use on individual systems.

With the usage of firewalls, protection levels may be set so that desktops are prevented from sending incomplete packets. Additionally, firewalls may be set so that the user must allow for outbound communication to occur. This would prevent participation in a DoS attack.

Conclusions

Risks can be managed in information systems environments. Security is an illusion as any system can be attacked under the right circumstances. Therefore, the greatest hazard is to be complacent.