SUBJECT

INFORMATION SYSTEMS PROJECT MANAGEMENT

TOPIC: SESSION 9: Information Systems Security

SESSION 9:Information Systems Security

Information Systems Security

I. Introduction
II. Issues concerning Information Systems Security
    A. Define IS security
    B. Why IS security is necessary?
    C. History and Back round of IS security
    D. Current issues concerning IS security
        1.) Spamming
        2.) Hacking
        3.) Jamming
        4.) Malicious software
        5.) Sniffing
        6.) Spoofing
        7.) Identity Theft
III. Solutions to contemporary IS security issues
    A. Solutions for "Spamming"
    B. Solutions for "Hacking"
    C. Solutions for "Jamming"
    D. Solutions for "Malicious Software"
    E. Solutions for "Sniffing"
    F. Solutions for "Spoofing"
    G. Solutions for "Identity Theft"
IV. The Future of Information Systems Security
    A. New technologies and techniques effecting the future of Information Systems Security
    B. Tips and information regarding maintaining a Secure Information System
    C. How security issues will continue to shape Information Systems Management

Introduction

Information Systems security is one of the biggest challenges facing society's technological age. Information Systems have become an integral part of everyday life in the home, businesses, government, and organizations. Information Systems have changed the way that people live their lives, conduct business, even run the government. Information Systems have become such an important part of everyday life because there are many uses of Information

Systems that make it much easier and faster to perform certain tasks, or even to perform certain tasks simultaneously.

Information Systems have become so developed and detailed in their short history. Society has developed along with the Information Systems, becoming a more technologically-reliable generation, also known as the digital firm era. Along with an increasing reliability for Information Systems, the digital firm era has also brought about an increasing profitability, competitiveness, and efficiency for any business of any size that uses an Information Systems.

Since the current technological generation has become so dependent upon Information Systems, the problems threatening Information Systems also threaten the order of everyday activities that many take for granted. The intricate role that Information Systems plays in daily activities has been developed near to perfection, but there are many current problems such as spamming, hacking, jamming, malicious software, sniffing, spoofing, and identity theft. These current problems are threatening the reliability and security of Information Systems.

With these current problems threatening Information Systems, users of Information Systems have been in the search for new techniques and new technology that will help fix the devastating consequences. Along with new techniques and new technology fixing these problems, users of Information Systems must also protect themselves. There are certain ways that users of Information Systems can protect themselves against all of the current problems. The future of Information Systems is somewhat unknown since it lies in the hands of the users. This unexpectedness also means with many unexpected problems that the users will have to solve.

The Issues

The problems which are facing information systems have either occurred through computer crime or computer abuse. Computer crime and computer abuse is widely becoming a widespread problem since technology can help accomplish almost any illegal or unethical task. There is a difference between computer crime and computer abuse, though; computer crime is when a person uses a computer to commit an illegal act, while computer abuse is when a person uses a computer to commit an unethical but not always illegal act.

Computer crime and computer abuse has become a widespread problem since the evolution of Information Systems. Before Information Systems were invented, data was protected more because most information was stored only in paper files, and only in certain departments of a business where many users would not have access to the data. With the evolution of Information Systems, large amounts of data can be stored in electric form rather than in paper files, so the data can be viewed by a larger number of users. Since more users can access the data electronically rather than manually, the data in turn, is more susceptible to the threat of computer crime and computer abuse.

Many businesses and individuals often feel serious effects from the following computer crime and computer abuse problems. Often at times, the users of Information Systems depend so heavily on the systems that a small setback will often cause huge setbacks for the business and individual. From a few minutes to a few days, the side effects of computer crime and computer abuse can be damaging to a business or individual who relies heavily on Information Systems to accomplish certain everyday tasks.

The current computer crime and computer abuse problems have threatened Information Systems due to the increased reliability of businesses and individuals on Information Systems, but also because of an increased risk of threat due to insecure telecommunication networks. Many of the ordinary threats to Information Systems such as hardware failure, fire, software failure,

electrical problems, personnel actions, user errors, and telecommunication problems also can lead to easier access to large volumes of data. When the telecommunication network itself is threatened, Information Systems of an individual or business becomes even more threatened.

One of the current computer crime and abuse problems threatening the future of Information Systems is spamming. According to Laundon, spamming can be defined as "the practice of sending unsolicited e-mail and other electronic communication." Spamming has become such a threatening problem with information systems because it is one of the cheapest and easiest methods to abuse a computer system. The spammers who send out all of these e-mails are only charged a few cents to send out the unsolicited e-mails to users who have not requested the information. There are laws prohibiting the use of spamming to abuse a computer system, but spammers rarely get punished since the laws are hardly enforced.

The next problem facing information systems is hacking. Hacking is when an illegal user tries to access private information that they are not entitled to access. This illegal access is done either by using Trojan horses, logic bombs, and many other types of software that can very easily be hidden. Sometimes the hackers will even go as far crashing an entire network. According to Laundon, "hackers flood a network server or Web server with many thousands of false communications or requests in order to crash the network." The repercussions from the attack of hackers can do serious harm to a business.

Jamming is also another computer crime and abuse problem that is threatening to information systems. It is not one of the most common, but it is one of the easiest to accomplish. The illegal purpose behind jamming is to find a way to tie up the lines to a computer is the central brain behind a website. Once the lines are tied up, then legitimate visitors can access the site, therefore, the lines are "jammed" with illegal users.

Malicious software is the most common form of computer crime against Information Systems. This computer crime occurs when computer viruses are sent through a means, usually the Internet, and these computer viruses "infect" the computer, often disabling programs or maybe even causing the computer to "crash," become inoperable. Once the computer virus is implanted into a computer's hard drive, it can be spread very easily, causing even more widespread damage. Some of the effects of computer viruses or malicious software are destroying programs, data, "crashing" a computer's operating system, clogging memory, etc. Again, if a business or individual receives a computer virus on their computer, the damage can be small to devastating.

Malicious software has become the most common form of computer crime because there are so many new computer viruses being spread. According to Laundon, "many thousands of viruses are known to exist, with two hundred or more new viruses each month." Some examples of damaging computer viruses are "Monkey", "Chernobyl", and "Code Red". The computer virus known as "Monkey" does not let the Windows operating system run, thus causing the hard drive disk to look like it is not working properly. "Chernobyl" is the nickname for a computer virus that infects a computer's files, and this computer virus ruins a computer's hard drive and ROM BIOS, which is the basic input/output system of a computer. "Code Red" is another computer virus that slows down the Internet and other computer processes. This computer virus is often spread as a "worm" as an attachment to an email, and then it hooks itself onto other computers once the email is sent, thus creating a very damaging chain-reaction.

Two more computer crime and computer abuse problems that pose a threat to Information Systems security are "sniffing" and "spoofing." "Sniffing" is a computer abuse problem which can let unauthorized users access private information about an individual because a piece of software can be used to cross the lines between an Internet user and a web site so the "sniffer" can

intercept sensitive data. "Spoofing" is somewhat like "sniffing," but "spoofing" involves the "spoofer" making a false web site geared to collect personal information from an Internet user to use it in criminal or unethical acts. The side effects of "sniffing" and "spoofing" are an increased risk of unsuspecting Internet users losing personal information. Once the personal information is collected, such as credit card numbers, social security numbers, birthdates, etc., the unsuspecting user is faced with a serious threat of misuse of that information, often resulting in horrible consequences.

Identity theft, a common computer crime, is the most common side effect of "sniffing" and "spoofing" and often times, the most horrible of all the computer crime and computer abuse problems. With an insecure Information System, identity theft often arises as a serious computer crime. Identity theft occurs, according to the Federal Trade Commission, "when someone possesses or uses [a person's] name, address, Social Security number, bank or credit card account number, or other identifying information without [a person's] knowledge with the intent to commit fraud or other crimes."

Identity theft can occur through a variety of low-technological and highly technological methods. Identity theft occurs through most businesses and organizations when illegal users gain access to stolen electronical records stolen from an employer. Identity theft vandals can also gain unauthorized access to records through bribery of an employer or someone in the business which has legal access to the records. Conning is also another way that illegal users can find information in a business or organization. The most common form of unauthorized access to computer is through hacking into an Information System of a business or organization. Once the information is illegally accessed, the results can be very harmful for the victim.

Solutions

These technological issues that have arisen pose many hindrances to the flow of meaningful information as well as security of information being sent. In spite of these impediments there are solutions to these problems. Some solutions come in the form of counter programming, others as legislation passed by various governing bodies. There is not, however, a single solution that solves or circumvents the issues the plague information systems and their security, each unique problem necessitates an equally unique solution.

The issue of junk e-mail or spamming is a point of much debate as to possible solutions. Currently many internet service providers offer policies against spamming and/or some sort of application that attempts to curb the amount of spam in user's mailboxes. America On-line, in particular, prohibits the sending of spam mail on their network cited laws such as the Computer Fraud and Abuse Act (18 U.S.C. 1030 et seq.) and the Virginia Computer Crimes Act (Va.Code Ann. 18.2-152.2 et seq.). Civil and criminal penalties may also apply to e-mail transmitted to the AOL Network in violation of the CAN-SPAM Act of 2003 (AOL, 1). Additionally they offer a "Spam Blocker" bundled with their main program which identifies some spam and prevents it from reaching their users accounts. MSN holds similar prohibitions regarding the sending of spam and uses Microsoft's "Smart Screen" technology to filter spam from their user's incoming mail (MSN, 1).

For some users the degree of protection presented by their internet service providers is insufficient and they seek alternative forms of spam prevention. These users are forming groups to lobby for anti-spam laws. These laws would prevent spam form ever being sent by attaching criminal charges to those found sending mass unsolicited e-mails. US Code 47.5.II, section 227 which is commonly known as "The Junk Fax Law" is a law prohibiting mass unsolicited faxes. Although much of the language in this law may seem to be applicable to computers and e-mail, the actual concept has yet to be tested in court or to

have firm ruling. New Jersey Congressman Christopher Smith has drafted a bill which modifies the junk fax law by including an electronic e-mail address of an individual in the existing prohibition against sending unsolicited advertising transmissions to fax machines. This law is truly 'opt-in' and is has a good deal support by consumers and internet service providers alike (Whitney, 2). In addition there are many completely new proposed laws circulating at the federal and state government levels which may completely solve the issue of spamming.

Hacking has remained a hot topic in the government for the better part of a decade. There are some preventative measures that can be taken by administrators or end users. On such preventative measure, a Firewall is a program used to closely monitor precisely what information passes in and out of a computer or information system. These programs can be set to keep other users out of to prevent information from leaving the computer or information system. The solution to dealing with these "cyber vandals", however, has been primarily found in the form of new legislation. There are a plethora of laws that deal with different types of hacking. The Computer Fraud and Abuse Act (as amended Oct. 3, 1996) is one such law; it covers subjects ranging from knowingly accessing a computer without authorization to intentionally causing harm to computers without permission. Unfortunately, there can be no true solution because as innovative as programmers become hackers will match their innovations and skill. The key to controlling this issue is to stay one step ahead of these hackers and to continually develop new and better forms of protection.

Jamming is an additional form of computer crime and abuse. Jamming can be prevented in a number of ways. The practice of jamming is considered illegal and is prosecuted under many of the same laws that govern hacking (i.e. The Computer Fraud and Abuse Act) (Manor, 5). The dilemma that makes jamming difficult to detect, prosecute and define is that it simulates actual web

page traffic. Most administrators will not regularly check the sources of most of the traffic to their sites (AOL Canada, 1). Additionally, when a jamming is noticed it is exceedingly difficult to trace the source or sources responsible for the act.

Sniffing, another form of computer crime and abuse is also difficult to detect. Sniffing can take one of two forms: Software which is downloaded either knowingly or unknowingly onto a computer or system, or physical in which a sniffing device is placed on the computer at the Ethernet port (Klaus, 6). Detecting sniffing software on a computers hard drive can be done using software designed to detect sniffing programs or they can be manually sought out by an administrator or user. As software is constantly being upgraded this can be difficult to do, though not impossible. If a physical sniffing device is used they can only be detected by a person physically checking the Ethernet connection of each individual machine. Penalties for this type of abuse also fall under the mesh of The Computer Fraud and Abuse Act.

Computer crime and abuse can also be seen in the form of spoofing also know as "phishing". This form of cyber crime is particularly current and harmful. These sites and e-mails are usually very well disguised and difficult to spot. Many instances of spoofing can be prevented by newer routers and firewalls (Jupiter Images). In instances where newer routers or firewalls are not available of should a site or an e-mail slip past these defenses there are some warning signs users can use to identify spoofing themselves. Some such signs are:

1. If the e-mail asks you for private account information or passwords.
2. If you are unfamiliar with the sender.
3. If the e-mail is unsolicited
4. Keeping your operating system and web browser up to date
5. Schedule spy ware protection software to run regularly on your computer

6. Run firewall software on your computer or ensure your home computer network is protected by a firewall-enabled network router.
7. Treat the links contained in any e-mails with suspicion. (four, 7)

Many say that the most rampant and dangerous form of computer crime is identity theft. Identity theft comes in many forms and levels. Identity theft can stretch from the theft of e-mail addresses from message boards, to stealing social security numbers, bank account numbers and passwords. Detecting identity theft is very difficult and prosecuting it can often be even more difficult. The best solution to identity theft is prevention. Keeping ones personal information close and guarding it well is the best solution to this problem. A person who has had their identity stolen or believes that they have should follow the subsequent steps:

1. Contact the fraud departments of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts, and all three credit reports will be sent to you free of charge.
2. Close the accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit when disputing new unauthorized accounts.
3. File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.
4. File your complaint with the FTC. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps us learn more about

identity theft and the problems victims are having so that we can better assist you (FTC, 9).

Computer abuse can also take the form of malicious software. There is a excess of programs designed to cause harm to computers and information systems. This software can take the form of viruses or worms that disable part of all of specific computers of entire systems. Software of a malicious nature can be prevented and detected by virus scans performed by programs made to detect such software. These scans can be performed regularly in a scheduled maintenance format or in a point of entry format wherein all removable disks, e-mails or incoming files are scanned as they are introduced to the computer (Whitney, 12). Virus scanning programs only work well if they are regularly updated with recent virus definitions.

Conclusion

As mentioned above, there are many current issues concerning Information Systems security. Some of these issues include spamming, hacking, jamming, malicious software, sniffing, spoofing, and identity theft; each one of these problems fit under one of two heading, computer abuse or computer crime. There are a lot of different techniques that some one can use to keep their information system safe from these crimes and abuse.

When you are dealing with spamming there are certain measures that you can take to guard your email account from spam. Spam is another term for unsolicited commercial email. Anyone that has an email account has at come point had an encounter with spam. Most people do not know how their email address got out to the people sending the spam; this is done through software called a Spambot. According to Scott Mueller, "a Spambot is a piece of software, a program that someone has written." Mueller describes the process of a Spambot like this "A Spambot starts out on a web page. It scans the page for two things: hyperlinks and email addresses. It stores the email addresses to use as targets for spam, and follows each hyperlink to a new page, starting the process all over."

There are various ways to hide your email address form these Spambots, but the easiest and best way to avoid spam is to not give out your email address. The trick is to leave your email visible to human visitor, but hidden from the spambots. There are many ways to do this according to www.spam.abuse.net/spam/, the most effective and simplest way to hide your email address is to make it into a graphic. Spambots cannot read graphics; in fact most of them cannot even load graphics, because it slows them down considerably. A graphic is just a jpg or a gif file that contains your email address in it. The only draw back to using a graphic is that the user must be bale to view the image to see your email.

Hacking is another large problem that information systems have to deal with today. The best, easiest, and lest costly way to stop someone from hacking on to your computer is to have a Firewall installed. HowStuffWorks.com says "A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through." Essentially, a firewall is a blockade to keep harmful forces away from your computer and personal information. There are three ways that a firewall can control traffic in and out of a network: Packet filtering, proxy server, and statefull inspection. Packet filtering is analyzing small pieces of information against filters. If the information does not make it through the filter then it is thrown out. Proxy server is when the firewall finds the information you need on the internet so that you are sure that the information is secure. HowStuffWorks.com states that Statefull inspection is "a newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded."

Malicious software is used to help people infect computers on the internet with viruses. There are tool kits that Microsoft and other companies have made that can stop cyber vandals from passing on viruses to your computer. Microsoft's Malicious Software Removal Tool is released once a month, it can according to the website, www.supportmicrosoft.com, "detect and remove current, prevalent malicious software. This malicious software includes viruses, worms, and Trojan horses."

Another computer crime is Sniffing. A Sniffer can be a self-contained software program or a hardware device with the appropriate software or firmware programming. They usually act as network snoops by examining network traffic, making copies of the data and possibly changing some of the content. This has become such a growing problem that the Federal Bureau of Investigation has had to design a sophisticated sniffer system called Carnivore. Carnivore's primary purpose is to intercept large volumes of electronic mail and other forms of electronic communication passing through a network (www.computerworkingabout.com).

An additional computer crime is spoofing. Ankit Fadia defines spoofing as a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming form a trusted hose. This is not hard for today's hackers to accomplish, all they have to do is find a "spoof" IP address of a trusted host then modify the header so it seems like it is coming from that host. Basically spoofers pretend to be and organization or person that they are not, so that they can get private information about the visitors of the website. Unless you are very knowledgeable on spoofing it is very difficult to catch or prevent. So, the best advice to give so you do not get spoofed is to be sure that the site you are on is a legitimate one. And be very cautious who you give your personal information, and credit card number to when on a website because you can never be too sure who you are actually giving it to.

Spoofing and identity theft go hand in hand when dealing with information systems. Identity theft occurs when someone steals your personal information without your knowledge to commit fraud or theft. They only need one of a few pieces of information to do so, such as your Social Security number, telephone calling card number, bank account or credit card number, or some other piece of your personal information for their own use. Many times

you do not even know that your identity has been abducted, usually people find out when they check their credit card bills (Sherman). Identity Theft Costs Americans over 5 Billion Dollars a year, with an average loss per victim of $10,000 (Sherman). Here are a few tips to preventing identity theft: Never carry documents with your Social Security number, or credit card number, never give them over the phone because you cannot be 100% sure who are you actually speaking with and because phone lines are easily taped. Also, do not write your Social Security number on your personal checks, and avoid using your Social Security number as an personal ID at your place of work.

Information Systems security is one of the biggest challenges facing our society the technological age. Information Systems have become an integral part of everyday life in the home, businesses, government, and private organizations. Information Systems have changed the way that people live their lives, conduct business, even how run the government. Information Systems have become such an important part of everyday life because there are many uses of Information Systems that make it much easier and faster to perform certain tasks, or even to perform certain tasks simultaneously. It the great abilities that this technology provides us we are burden with an ethical and moral obligation to manage and control ourselves as well as others for the greater good of man kind.