Global Information Assurance Certification Paper

CyberCrimes
Norma Vanessa Ruiz
December 20, 2001

Introduction

Computers control communications, power delivery, emergency systems, financial services and aviation to name a few. They are used to educate and to store vital information. The uses of computers and the Internet are endless in today's society. The September 11th attacks have raised concerns that terrorists might target the nation's information systems for the sole purpose of disrupting our lives. After September 11 companies have realized that the worst-case scenario can become a reality and have pushed their agendas aside to discuss ways to keep their systems "safe". Companies not only in the United States but also in South America, Asia and Europe are seeking more help than before to survive a disaster.

We depend on computers and therefore we are at risk. There are as many predators in cyberspace as there are anywhere else. The modern thief can steal more with computers than with a gun. "A hacker can use a remote terminal or their home computer to seize control of electric power, shut down the operation of financial institutions and disrupt emergency telecommunications systems using technology that is already available in the market." [1]

What is a cybercrime? "Cybercrime is one of the fastest evolving areas of criminal behavior and a significant threat to our national and economic security."[2] There is a major threat to our national security posed by networked computers, especially through the Internet. Cybercrimes are growing exponentially and could dangerously impact our lives.

Cybercrimes

Computers cannot kill or injure a person directly, but this does not mean that it can't risk human lives and the economy indirectly. The most significant risk is our economy. For example, if some groups target several large phone networks at once, the results will be devastating to the economy of our nation.

> The mafia uses computers for extortion. Drug dealers enlist an encrypted fax machine to send orders for narcotics to their suppliers in Columbia. Prostitution rings maintain their customer payments and client lists through computer software applications. Burglary rings track break-ins and then inventory their winnings from each job. Organized crime profiteers call for a hit on a potential witness staying in a hospital. Instead of physically carrying out the dirty deed, they crack the hospital's computers to alter the dosage of medication.[3]

Cybercriminals can range from teenagers who vandalize web sites to terrorists who target a nation and everything in between. Some Cybercrimes include but are not limited to:

- Computer related fraud, forgery and scams. Cyberfraud offers nonexistent goods, information or services to customers with the purpose of transmitting the victim's funds to their pockets.

Major Internet Scams
  - Web Auctions
  - Internet services
  - General merchandise
  - Computer equipment/software
  - Multi-level marketing schemes
  - Business opportunities/franchises
  - Work- at- home plans
  - Credit card issuing prizes/sweepstakes
  - Book sales
  - Stock manipulation

- Online sexual exploitation of children and child pornography including downloading, reproduction and distribution of prohibited material.
- Reproduction and distribution of copyright protected material, software piracy and intellectual property theft. This is relatively easy and usually only large rings of distributors are caught.
- Unauthorized access (hacking) violations. Network intrusions, where an unauthorized user penetrates into network computers where he/she is not authorized. System intrusion creates a wide variety of security concerns. Hacked systems can be used for information gathering, information alteration, and sabotage. Vulnerabilities exist in almost every network. Hackers sometime crack into systems to brag about their abilities to penetrate into unauthorized systems, but others do it for financial gain or other malicious purposes. Today Hacking is simpler than ever, hackers can now go to web sites and download protocols, programs and scripts to use against their victims.
- Emanation Eavesdropping. Receipt and display of information, through the interception of radio frequency signals.
- Denial of service attacks. In these cases hackers use tools such as Tribal Flood Net (August 1999), TFN2K (January 2000), Trinoo (June 1999), or Stacheldraht (German for barber wire)(October 1999) on a number of systems. When the hacker sends a command, the victim's system starts to send messages against a target system. The target system then is overwhelmed with the traffic from the hacker and is unable to function causing users that try to access the systems denied services.
- Malicious code (viruses, worms and Trojan horses). Malicious code has turned more into worms. These exploit security and vulnerabilities and cost millions of dollars to companies and government agencies. Worms are different than viruses because they are able to spread themselves with no user interaction. A virus can attack systems in many ways: by erasing files, destroying hard disk drives and corrupting databases. Trojan Horses are independent programs that when called by an authorized user perform useful functions but at the same time performs unauthorized functions. Some well know examples of malicious code are the Melissa Macro Virus, the Morris Worm, and the Trojan horse Back Orifice 2000. For example, the Melissa Micro Virus created by David L. Smith cost $80 million in damages.
- Social Engineering. Using social skills to obtain information, such as passwords and pin numbers to be used in an attack against computer systems. [4]

- Password cracking and theft. These are much easier with powerful computer searching programs and password sniffers that can match numbers or alphanumeric passwords to a program in a limited time.
- Cyber stalking. The goal of a cyber stalker is control. Stalking and harassment over cyberspace is more easily practice than real life. Sometimes the harassment starts with threatening messages of hate and obscenities. This situation can escalate to the point where the harasser traces the person's phone number and address causing the person to face physical danger. There are many cases where cyber stalking crosses over to Real Life Stalking.

  Some examples of computer harassment are:

  1. Unsolicited and threatening e-mail
  2. Live chat obscenities and harassment
  3. Hostile postings about someone
  4. Spreading vicious rumors about someone
  5. Leaving abusive messages on site guest books
  6. Online impersonation
  7. Electronic sabotage (sending viruses etc)

- Spoofing of IP addresses. Inserting a false IP address to impersonate an authorized user.
- Cyber Vandalism.
- Industrial Espionage. Corporations love to spy on other companies and with network systems this can be an easy task. Companies can retrieve sensitive information rarely leaving behind any evidence. Cyberespionage can also be applied to nations that spy on other countries sensitive information.
- Insider threat. Insiders of companies, government and universities do most of the unauthorized access. Insiders commit 71% of unauthorized access cases. Insiders do not need a great deal of knowledge about computer intrusions, because their knowledge from inside already allows them to gain unrestricted access to steal information or cause damage. These intrusions are sometimes hard to fight since companies do not expect attacks from their employees.
- "Hacktivism, refers to the marriage of hacking and activism. It covers operations that use hacking techniques against target Internet sites with the intent of disrupting normal operations but not causing serious damage."[5] These attacks are politically motivated, especially aimed to government agencies so the attacker's voice can be heard.
- Cyberterrorism. "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents."[6]

Case History of Cybercrimes

Theft of credit card numbers, proprietary information or government sensitive material threatens not only the economy but also our national security. There are hundreds of cases of Cybercrimes that cannot be discussed in detail on this paper. These not only interrupt our daily lives or appear on the headlines of the newspapers, but also affect our economy and threatening of our national infrastructure.

“Imagine a virus on the computer system of a hospital. Human lives are at risks, making that virus a tool of murder no less dangerous than that of a loaded weapon.”[7]

“On August 17, 1999, a Trinoo network of at least 227 systems was used to flood a single server at the University of Minnesota, including more than 100 compromised computers at the University of Washington. The attack rendered the system inoperable for two days.”[8]

“Terrorists could use software attacks to disable ICANN's 13 ``root'' server computers around the world. Each of the servers is the foundation of an Internet domain suffix, such as .com, .org or .gov. Such an attack could render the Internet or parts of it useless.”[9]

“Testimony before a Senate committee confirmed that during April and May of 1991, computer hackers from the Netherlands penetrated thirty-four Department of Defense computer sites.”[7]

Recently charity scams related to the September 11th terrorist attacks have been carried out through e-mail, in these cases solicitors are pretending to be from The Publisher’s Clearing House or the American Red Cross.

The examples are endless, from pro-US hackers interrupting Middle Eastern Web Sites to anti-US hackers penetrating our government sites. From hackers diverting 911 calls to pizza parlors to teenager hackers shutting down aviation administration control towers.

Cyberlaw

There is a difference between hackers who break into a web site to paint mustaches on pictures and cyberterrorists who go to these same web sites with the purpose of causing harm and damage. Law enforcement has many challenges when we talk about cybercrimes. First there is the identification of the criminal and its jurisdiction. Second, there is not enough trained personnel or equipment to fight against these computer crimes.

One of the major difficulties that distinguish cybercrime from other crimes is the identification of your attacker. The WHO, WHAT, WHEN, WHERE, and WHY of cybercrime is difficult to address. Cybercriminals today use encryption, which makes law enforcement work complicated, plus their attacks travel through various networks in many countries before hitting their ultimate target.

> Almost every federal agency within the U.S. has some division responsible for computer security. But the preeminent agencies of the field are still the agencies charged with national security, such as the National Security Agency, the Central Intelligence Agency, the Federal Bureau of Investigation, and the Justice Department and the Secret Service within the Treasury Department. It is important to acknowledge that it is the character of these agencies, their histories and their other responsibilities that give the subject of computer security in the United States a particular kind of atmosphere, largely that of the military and national security community. [10]

The security of our information systems must be continually increased. The agencies responsible for our nation's security should be more proactive instead of falling behind with the great growth of cybercrimes. Encryption will be a critical component to secure computer systems and information transfers in the future. At the same time these encryption techniques allow criminals to encrypt their data and become difficult for computer forensics, law enforcement and intelligence agencies to gather intelligence from communication intercepts. While cybercriminals continue to disrupt government agencies and companies, the law struggles to catch up with an increasingly complex, networked world progressing at an exponential rate.

The lack of law enforcement in cyberspace is a big issue. Finding cybercriminals especially in other countries can be tougher than finding out who is sending anthrax through the mail. Although most countries agree that child pornography is a crime, they do not share the same ideas on Internet based gambling or cyberstalking as we do. Not realizing the damages and risk of life in some cases, countries view hackers and other cybercrimes as a moral issue and not a crime.

Crimes committed in cyberspace raise difficult legal questions of Jurisdiction. A typical cybercrime investigation involves multiple states and in some cases multiple countries. It is already hard in the United States to perform investigations involving different states or jurisdiction. Imagine how hard it is to work with other countries, which in some cases do not have adequate cyberlaws and not enough trained personnel to deal with the investigation.

How can cybercrimes be prevented?

This is a hard question to answer. The most secure defense against cybercrime is to make sure computers that run critical infrastructures are not physically connected to any other computers that are possibly connected to the Internet.

These steps are important for our security:

1. Maintain clear and consistent security policies and procedures.
2. Vulnerability assessments to identify weaknesses and ensure audit trails are on.
3. Installed software and hardware to recognize attacks. Use of firewalls, encryption, virus detection, smart cards.
4. Require the use of alphanumeric passwords and change login passwords frequently.
5. Mandatory correction of identified problems.
6. Mandatory reporting of attacks to help better specify weaknesses and communicate vulnerabilities necessary for corrective actions.
7. Incident response capability to aggressively detect and react to track and prosecute attackers.
8. Damage assessments to re-establish the integrity of information compromised by an attacker.
9. Awareness training to ensure computer users understand security risks.
10. Assurance that security personnel have sufficient time and training to perform their duties.
11. Maintain backups of all important data and original operating system software.

Security is essential for our systems and we recognize that security costs money. Hardware, software and services to make web sites secure will be more than double the cost it was last year. This spending is justified because of the need to maintain a secure infrastructure and economy.

Conclusion

America must defend its cyberspace. This can only be done if government and industry work together. Our information is fragile and vital. The military should be able to define its security needs and work with the private sector to meet them. This sharing of information will benefit the government and private sectors. We may not be able to prevent denial of service attacks completely, but we must explore ways to encourage industry and government to share information in order to prevent such attacks.

Protecting our nation's critical infrastructure starts with you. By educating yourself about computer security and the ethical use of computers. Companies should continue their efforts to educate their employees, encouraging them to communicate security matters between departments and organizations. Computer security personnel should maintain infrastructure integrity by implementing software updates and the latest software patches.

To deal with the future, we need to improve our ability to protect our systems and understand our adversary's forces, capabilities and intentions. Catching and punishing those who commit cyber crimes is essential for deterring future attacks. When a cyber attack occurs, it is not initially apparent whether the perpetrator is a mischievous teenager, professional hacker, a terrorist group, or even a hostile nation. Law enforcement must be equipped with the resources and the authority necessary to trace a cyber attack back to its source and appropriately prosecute.

References

1. Wallace, Bill. "Experts Warm of Cyberterror Threat (11/13)." Hot Topics. c.2001 San Francisco Chronicle. URL: http://www.computernewsdaily.com/ (December 17, 2001)
2. Freeh, Louis J. "Cybercrime." Congressional Statement. February 16, 2000. URL: http://www.fbi.gov/congress/congress00/cyber021600.htm
3. Armstrong, Illena. "Investigators Focus on Foiling Cybercriminals." Computer Forensics. April 2000. URL: http://www.scmagazine.com/scmagazine/2000_04/cover/cover.html
4. Krutz, Ronald. Vines, Russell. The CISSP Prep Guide. Canada: John Wiley & Sons, Inc., April 2001. Page 298
5. Denning, Dorothy E. Activism, "Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." URL: http://www.nautilus.org/info-policy/workshop/papers/denning.html (December 12, 2001)
6. Pollitt, Mark M. "CYBERTERRORISM - Fact or Fancy?" URL: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html (December 12, 2001)
7. Devost, Matthew G. "NATIONAL SECURITY IN THE INFORMATION AGE." May 1995. URL: http://www.terrorism.com/documents/devostthesis.html
8. Sinrod, Eric J. Reilly, William P. "Cyber-crimes: A Practical Approach to the Application of Federal Computer Crime Laws" URL: http://www.taoiw.org/resources/cybercrime1.html (December 17, 2001)
9. Keefe, Bob. "Internet group reviewing vulnerability to terrorism (11/13)."Hot Topics. c.2001 Cox News service. URL: http://www.computernewsdaily.com/
10. Chapman, Gary. "National Security and the Internet." July 1998. URL: http://www.utexas.edu/lbj/21cp/isoc.htm