BADM590

May 1

2008

IT Governance

Final Project

~ Cyber Crime ~

Student: Kuo-Liang Chen

Instructor: Dr. Michael Shaw

Table of Contents

Cyber-Crime

Unlike most of traditional crime, cyber-crime doesn’t need a physical contact between victim and criminal. Even the criminal can attack the victim from the other side of the world. Cyber-crime can’t be restricted by time and distance and its damage may be as huge as anyone can image. In a current issue of *BusinessWeek*, a special report of cyber-espionage states the issues of series cyber-attacks to the U.S. government. Also, some authorities suspect that the attack might potentially be supported by governments such as Russia and China.

The cyber crime is not only intimidating individuals but also threading companies and governments. For governments, the losing control of cyber crime may result in a damage of state security and suspecting of international relationship. Companies may also endanger their reputation and property, if they can not efficiently avoid the cyber attacks.

The Characters of Cyber Crime

The cyber crime has three important character distinguishing from the traditional crime.

1. **No limitation of time and distance:** As mentioned before, the attackers can scan and attack the IT equipment and infrastructure in anywhere on the Earth.
2. **No physical contact: T**he hackers do not need to see you and you won't see the hackers also. However, they can attack you whenever you lose your defense.
3. **Sometimes unawareness: Since not everyone has the sufficient knowledge of cyber crime, it is easy that the victims who are without the awareness of the suffering crime.**

IT Technology and Cyber Crime

After the introducing of IT technology, people's lives have been into the information era. Computers, laptops, and internet are becoming one of the most important stuff for people's daily activities. People check email all the day; talk to friends on-line; search information through the internet.

For companies, they depend heavily on ERP system and B2B platforms to increase the efficiency of operation and communication. Even many of companies use VoIP to cut the cost of phone bill. And, some companies use the virtual technology for meeting with other colleagues around the world.

Governments also employ IT technology to serve as a critical role to enhance not only the power of military but also the efficiency of public services. In Iraq's war, we saw the extremely example of information technology employed by military. By the assistance of IT technology, air force can destroy any target precisely, which can eliminate the unnecessary death and damage. Soldiers can immediately know what is they location and where is the target by the GPS systems. Generals can coordinate their army simultaneously by a combination of IT technology including internet, GPS, and server computers etc…

However, the more dependent on IT technology, the more likely the IT technology will treat people if it is used by evil ways. Unfortunately, not only the Microsoft operation system itself has many defects of security but also the internet has so many ways that hackers can take advantages of their knowledge to penetrate the protective infrastructure. Hence, it will treat every people if we do not have good preparation to

prevent our IT equipment and systems from being attacked by hackers.

Some hackers are only feeling that it is interesting to do some tricks to suffer other people. The others, however, may be supported by some organization to attack the internet or IT infrastructure on purpose. If the attacks are on purpose, it is really hard to track back those attacks and define who behind those attacks and where are them.

Types of Cyber-Attack

Web vandalism:

A normal attack to deface the webpages, which causes a little harm but most of amateur hackers like to do it.

***Propaganda*:**

Some hackers spread political messages to anyone who accesses to the internet.

Gathering data:

Hackers intercept and modify the insecurely handled information. This is an attack that threatens seriously for both companies and governments. Company may lose its customers confidential data such as credit card number and personal information.

Governments may face the threat of missing defense secrets and military data. There are some notorious attacks i.e. Titan Rain and Moonlight Maze.

Distributed Denial-of-Service Attacks:

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is trying to make some computer resources becoming unavailable to its intended users. The damage of DoS attack is obvious and immediate. A user who is suffered by DoS attack can immediately find his or her IT equipment becoming inefficiency and even malfunctioning and the harm may be temporary or indefinite.

Equipment disruption:

Some of military activities related to IT and satellites for co-ordination will most likely to be the target of this kind of attack. The military orders and communications will be intercepted and modified. It is dangerous that soldiers are exposed to a position that might cause unnecessary conflict and loss.

Attacking critical infrastructure:

The criminal might shot down the important infrastructure like power, water and transportation. A movie performs that a group of criminal try to ask the government

pay them a huge amount of money and threaten to shot down the entire infrastructure in the country.

The Recorded Cyber-Attacks

Solar Sunrise:

In February, 1998, a series of DoD attacks stoke Air Force, Navy, and Marine Corps. Solar Sunrise (n.d., 1998) says that “The attack pattern was indicative of a preparation for a follow-on attack on the DII. DoD unclassified networked computers were attacked using a well-known operating system vulnerability. The attackers followed the same attack profile: (a) probing to determine if the vulnerability exists, (b) exploiting the vulnerability, (c) implanting a program (sniffer) to gather data, and (d) returning later to retrieve the collected data.”

The report of damage maintains that no classified data had been stolen. However, these attacks occurred when the U.S. was preparing for potential military action against Iraq due to UN weapons inspection disputes and could have been aimed at disrupting deployments and operations. The systemized process of attack drew the attention to the

possibility of state governments or terrorism behinds them. (Solar Sunrise, n.d., 1998)

Moonlight Maze:

This is the U.S. government's designation for a series attacks on American computer system between March, 1998 and 1999. The attackers used a special code to access and pass to websites at the Defense Department., NASA, the Energy Dept., and weapons labs across the United States. They stole a huge amount of data related to naval codes and missile guidance systems. However, U.S. government can only track the attack back to Moscow but can not make sure whether the origination from Moscow. Moscow also denied any involvement of these series of attacks.

Titan Rain:

This is a series of cyber-attacks blamed on China in origin and a U.S. government designation of these more complicated attacks. Titan Rain consists zombie computer, spyware and virus infection as well as masked by proxy. The motivation of these attacks, however, remains unknown. The attacks may caused by state-sponsored espionage, corporate espionage, or random hackers.

The intrusions were discovered by Shawn Carpenter, a cyber security analyst at Sandia Labs. After the institution reported to U.S. Army and FBI, Sandia fired this guy. Later, Carpenter filed a suit to accuse Sandia of wrongful termination. Finally, he received a jury award of $4.7 million in Feb., 2007.

Byzantine Foothold

2007, some more sophisticated attacks stroked U.S. from State Departments to Boeing and firstly was detected by Booz Allen Corp. Military cyber security authorities suspect there are some nation-state resources behind those attacks. The U.S. government launched a defense emergency program called Byzantine Foothold. BF specifically aimed at curbing and preventing foreign intrusions into the cyber networks of U.S. government and its agencies as well as some of the largest military-industrial contractors.

The Influences of Cyber-Crime

Individual:

For individual network users, the cyber-crime may cause you some inconveniences such as shutting down the system, decreasing the efficiency, and crashing the personal

internet. The damage is relative smaller and easy to be amended excepting some important information such as ID, password, and credit card numbers. Specialists suggest that people should use their personal information more carefully and only use them under the secured web environments.

Business:

The cyber-attacks can cause more serious loss of business. Since most of company use some servers to be the gateway to filter out the potential crime and attacks. Thus, if the hacker crashes the protection, the internal computers will easily be infected and destroyed completely.

Moreover, the customers' data may be stole at the same time. It is a serious crisis of losing customers' personal information since customers will lose their trust in this company. Therefore, the customers may not come to the company anymore.

Government:

It is most dangerous that government is suffered by the cyber-attacks. The related departments are important for most of people living in the country. Thus, if the attackers invade into the government cyber system, it will be a great threat for the

general public. The attackers can terminate the transportation system, shut down the power plant, and modify or steal the military data. As I mentioned before, if the military data is modified by the wrong information, it will be dangerous for the soldiers and maybe cause disputes among countries.

Laws and Regulations

Computer Fraud and Abuse Act:

The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1984 intended to reduce "hacking" of computer systems. It was amended in 1994, 1996 and in 2001 by the USA PATRIOT Act. (Copyright 2001 4th Edition, Computer Confluence: Prentice Hall Books, written by George Beekman.)

The USA PATRIOT Act increased the scope and penalties of this act by:

1. Raising the maximum penalty for violations to 10 years (from 5) for a first offense and 20 years (from 10) for a second offense;
2. Ensuring that violators only need to intend to cause damage generally, not intend to cause damage or other specified harm over the $5,000 statutory damage threshold;

3. allowing aggregation of damages to different computers over a year to reach the $5,000 threshold;
4. Enhancing punishment for violations involving any (not just $5,000) damage to a government computer involved in criminal justice or the military;
5. Including damage to foreign computers involved in US interstate commerce;
6. Including state law offenses as priors for sentencing; and
7. Expanding the definition of loss to expressly include time spent investigating and responding. This is why it is important for damage assessment and for restoration. (Theofel v. Farey Jones, 2003)

The Fraud Act 2006:

The Fraud Act 2006 (2006 c.35) is an Act of Parliament in the United Kingdom, affecting England and Wales and Northern Ireland. It was given Royal Assent on 8th November 2006, and came into effect on 15th January 2007. The Act gives a statutory definition of the criminal offence of fraud, defining it in three classes:

1. Fraud by false representation
2. Fraud by failing to disclose information
3. Fraud by abuse of position.

"Fraud by false representation" is defined by Section 2 of the Act as a case where a

person makes "any representation as to fact or law ... express or implied" which they know to be untrue or misleading. "Fraud by failing to disclose information" is defined by Section 3 of the Act as a case where a person fails to disclose any information to a third party when they are under a legal duty to disclose such information. "Fraud by abuse of position" is defined by Section 4 of the Act as a case where a person occupies a position where they are expected to safeguard the financial interests of another person, and abuses that position; this includes cases where the abuse consisted of an omission rather than an overt act.

In all three classes of fraud, it requires that for an offence to have occurred, the person must have acted dishonestly, and that they had to have acted with the intent of making a gain for themselves or anyone else, or inflicting a loss (or a risk of loss) on another.

It provides that a person found guilty of fraud was liable to a fine or imprisonment for up to twelve months on summary conviction (six months in Northern Ireland), or a fine or imprisonment for up to ten years on conviction on indictment. This Act largely replaces the laws relating to obtaining property by deception, obtaining a pecuniary advantage and other offences that were created under the Theft Act 1978. These offences attracted much criticism for their complexity and difficulty in proving at

court. Much of the Theft Act 1978 has been repealed, however, the offence of making off without payment, defined under section 3 has not been affected. (The Fraud Act 2006)

Act to strike back

The hackers are using any possible vulnerability to crash people's computers. How to protect our computers and prevent them from cyber crime comes to be a public issue. Here are some suggestions for future act to strike against the cyber crime. Those suggestions are applied for individual, business, and government.

Cut connections

To cut down the number of portals which have potential threat of cyber attack can eliminate or decrease the channel available for hackers to knock the system and crash it.

Passive intrusion prevention

For the first defend, we can set a plan to indentify when unauthorized entities have gained access to computer network. One of the guest speakers mentioned the same

idea in IT governance. For IT governance prospective, building an authorizing control system can prevent the unauthorized actions which may result in a failure of control.

Active intrusion preventions

An initiation of tracking back program can help find out the origin of attacks. This program can improve the knowledge of who are the potential threats and turn out to be a strategy of vulnerability management.

Education

The IT technology is sort of a dilemma that it helps people to increase the productivity and to change the living style but it also threatens the national and personal security. Therefore, education can not only direct people to use the technology in the positive way but also improve people's knowledge of IT crime and further understand how to protect them from being attacked.

Critical infrastructure protection

To focus the efforts on the main internet service providers (ISP) and other important internet companies to build a strong protection among these points can efficiently avoid most of the attacks to invade into internet.

Cyber R&D

Investing the innovation of new technology in IT R&D to improve the skills of vulnerability management can help defend the abnormal activities and intentional attacks.

Conclusion

The internet and IT technology is a growing phenomena that brings industrialization into a new era. It is also one of the most important innovations in the late decades. The IT technology drives some of the social revolution such as the e-Government, business automation, and pervasion of personal computer. People are benefited by this tremendous tread and innovation.

However, IT technology also threatens us many ways. Other than the cyber crime, the internet provides too much information that people may not able to learn. The pressure from learning new knowledge forces people work harder and harder for not being sunk by the information flood. Meanwhile, the new type of online entertainments may attract people to spend too much time on those games and virtual

societies. People will sometimes be confused by virtual world and real world.

Although IT technology is important for contemporary world, everyone should aware the potential threats from IT technology if it be employed by evil ways. A good preparation of preventing the cyber crime is critical to protect the IT infrastructure. Education can play a key role to teach people to distinguish good usages from bad applications. The fundamental improvement of IT knowledge can ultimately build the consensus of fighting cyber crime and future development of defending technologies. We should keep in mind that technology can benefit people only when it is employed by the positive ways.

Reference

A guide to computer crime by Watson Business Systems Ltd
http://legal.practitioner.com/computer-crime/

Brian Grow, Keith Epstein, Chi-Chu Tschang, & Jonathon Rosen (2008, April 21) "The new E-Spionage Threat." *Businessweek*, 33-41

"Cyber Crime: A 24/7 Global Battle", Mcafee. Retrieved on 2007-11-30.
http://www.mcafee.com/us/research/criminology_report/default.html

Graham, B (2005). "Hackers Attack Via Chinese Web Sites", Washington Post, August 25, 2005.

Jonathan V. Post (1979), "Cybernetic War," Omni, pp.44-104, reprinted The Omni Book of Computers & Robots, Zebra Books, ISBN 0-8217-1276

Moonlight Maze (n.d.) from http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/

Shaun Waterman (Sep. 2007), UPI Homeland and National Security Editor, “China 'has .75M zombie computers' in U.S” .United Press International. http://www.upi.com/International_Security/Emerging_Threats/Briefing/2007/09/17/china_has_75m_zombie_computers_in_us/7394/

Solar Sunrise (n.d.) from http://www.globalsecurity.org/military/ops/solar-sunrise.htm

The Fraud Act 2006 (Commencement) Order 2006 - SI 2006 No. 3200 (C.112) ISBN 0-11-075407 7

Theofel v. Farey Jones, 2003 U.S. App. Lexis 17963, decided August 28, 2003 (U.S. Court of Appeals for the Ninth Circuit). Using a civil subpoena which is “patently unlawful”, “bad faith” and “at least gross negligence” to gain access to stored email is a breach of this act and the Stored Communications Act.