An overview: Anti-Cybercrime Efforts in Taiwan

Chien, Shih Chieh
An overview: Anti-Cybercrime Efforts in Taiwan

Chien, Shih Chieh
Investigator of MJIB
Taiwan
m36030@mjib.gov.tw

The efforts in preventing and investigating cyber-crime in Taiwan have been receiving considerable attention all over the world. As a matter of fact, special task forces, such as the Cyber Crime Investigation Unit of Investigation Bureau have been set-up to fight cybercrime in Taiwan in the recent years. Even though, it is still insufficient to deal with so many cybercrime cases. Therefore, we proposed some basic solutions to the cybercrime problems, which is a view to introduce the effort of the Cyber Crime Unit of Investigation Bureau to battle with cybercrime on the Internet.

. Introduction
The Internet population has been growing much faster than the total population. The numbers of cybercrime cases and suspects have been increasing much faster than even the Internet population and reached a record high in 2006. Also, cybercrime suspects are becoming younger. Cybercrime is conducted by highly educated people. The efforts in preventing and investigating cyber-crime in Taiwan have been receiving considerable attention all over the world.

As a matter of fact, special task forces, such as the Cyber Crime Investigation Unit of Investigation Bureau have been set-up to fight cybercrime in Taiwan in the recent years. Even though, it is still insufficient to deal with so many cybercrime cases. Therefore, we proposed some basic solutions to the cybercrime problems, which is a view to introduce the effort of the Cyber Crime Unit of Investigation Bureau to battle with cybercrime on the Internet.

. Fighting Cybercrime in Taiwan
With the explosive growth of the Internet worldwide, computer crimes increasingly are prone to have international dimensions.

In addition to MJIB, the Ministry of Justice has established a Cybercrime Prevention and Fighting Center in Prosecutors’ Office.

Based on the Ministry of Justice statistics, in 2006 prosecution of computer crime cases were 2118 in total, subject to Offenses of Interfering with the Usage of Computers Chapter 36 (Chapter 36) were 74 cases; convicted were 1428 cases, subject to Chapter 36 were 26 cases.
In 2007, prosecution of computer crime cases were 2406 in total, subject to Offenses of Interfering with the Usage of Computers Chapter 36 (Chapter 36) were 54 cases; convicted were 2250 cases, subject to Chapter 36 were 28 cases.

In 2006 and 2007, compared to the overall prosecution of computer crime cases, 13.6% growth in 2007, subject to Chapter 36 has dropped 27%; Overall computer crime conviction cases, 57.6% growth in 2007, Chapter 36 is 7.7% growth.


. An introduction of Chapter 36 of Criminal Law and Frequently Used Statutes

A. Chapter 36 of Criminal Law: Offenses of interfering with the usage of computers

1. Article 358:
   A person who accesses another's computer or related facilities without justifiable causes by logging in another's password, deciphering the protective measures for the use of computers, or exploiting a computer system loophole shall be punished with imprisonment for not more than three years, detention, or a fine not more than 100,000 yuan may be imposed.

2. Article 359:
   A person who obtains, deletes or alters the electromagnetic records in another's computer or its related facilities so as to cause damage to the public or another shall be punished with imprisonment for not more than five years, detention, or a fine not more than 200,000 yuan may be imposed.

3. Article 360
   A person who interferes with another's computer or related facilities by making use of computer programs or other electromagnetic means without justifiable causes shall be punished with imprisonment for not more than three years, detention, or a fine not more than 100,000 yuan may be imposed.

4. Article 361
   A person who commits offenses as set forth under articles 358, 359 and 360 against a government agency' computer and related facilities may be punished for such an offence increased by one second.

5. Article 362
   A person who designs computer programs especially for committing the offenses as set forth under chapter 36, and these computer programs shall be used for committing these offenses by oneself or someone else so as to cause damage to the public or another shall be punished with imprisonment for not more than five years, detention, or a fine not more than 200,000 yuan may be imposed.

6. Article 363
Prosecution for an offence as set forth under articles 358, 359 and 360 may be instituted only upon complaint.

B. Frequently Used Statutes

The following statutes are used most frequently by the MJIB to investigate computer-related crimes.

1. Chapter 36 of Criminal Law as mentioned above: Offenses of interfering with the usage of computers.
6. Chapter 32 of Criminal Code (Fraud Crimes Chapter): Mail Fraud and Wire Fraud.

- How the MJIB investigate computer crime?

This paragraph provides information about the investigative and prosecutorial process for computer crimes and explains some of the resources the MJIB uses when it investigates computer crime.

A. CIU and CFL

MJIB use sophisticated methods to investigate and coordinate cyber incidents. In the Taiwan, the Cybercrime Investigation Unit (CIU) is a division under the MJIB. CIU processes complaints of cyber crime and then coordinates computer crime investigations.

The MJIB’s Cyber Division at MJIB Headquarters in Taipei coordinates investigations in which networks or computers are exploited as instruments in criminal activity or as targets. High priority is given to investigations that involve terrorist organizations or intelligence operations sponsored by foreign governments. The MJIB trains computer investigators who work in MJIB field offices to investigate cyber crimes.

The MJIB maintains a computer forensic laboratory (CFL) at MJIB Headquarters in Taipei for advanced data recovery and for research and development. Technology has made it easier for criminals to hide information about their crimes. Because of the sophistication of the digital environment, evidence is collected and handled differently than it was in the past and often requires careful computer forensic investigation. CFL is a one-stop, full service forensics laboratory and training center devoted entirely to
the examination of digital evidence in support of criminal investigations. Four MJIB field offices also have specialized cyber squads called Cyber Action Teams which major duties is to investigate cyber crimes and to aid cybercrime investigations.

B. Cyber crime investigation

Computer crimes can be separated into two categories:

1. crimes facilitated by a computer;
2. crimes where a computer or network is the target.

When a computer is used as a tool to aid criminal activity, it may include storing records of fraud, producing false identification, reproducing and distributing copyright material, collecting and distributing child pornography, and many other crimes. But first category of computer crimes is not the major duty of CIU. CIU only investigate the crimes which belong to Chapter 36 of Criminal Law in Taiwan unless super agency asks CIU to investigate.

Crimes where computers are the targets can result in damage or alteration to the computer system. Computers which have been compromised may be used to launch attacks on other computers or networks.

The MJIB uses a number of statutes to investigate computer crimes. The MJIB is sensitive to the victim's concerns about public exposure, so any decision to investigate is jointly made between the MJIB and the Prosecutor in order to safeguard the victim's fundamental human rights.

C. Gathering information

Those organizations will be recommended to follow these steps and assist law enforcement agencies in their investigation:

1. Preserve the state of the computer at the time of the incident by making a backup copy of logs, damaged or altered files, and files left by the intruder.
2. If the incident is in progress, activate auditing software and consider implementing a keystroke monitoring program if the system log on the warning banner permits.
3. Report the incident to the CERT. Consider authorizing them to release the incident information to law enforcement.
4. Document the losses suffered by your organization as a result of the incident. These could include the
   - estimated number of hours spent in response and recovery.
   - cost of temporary help
   - cost of damaged equipment
   - value of data lost
   - amount of credit given to customers because of the inconvenience
   - loss of revenue
value of any trade secrets

5. Contact law enforcement, provide incident documentation, share information about the intruder, and share any ideas about possible motives.

D. Contact Information

To initiate an investigation, contact your local MJIB office or another appropriate law enforcement agency. To report an incident to the MJIB, you see the website "http://www.mjib.gov.tw".

Conclusion

Cybercrime Investigation Unit of Investigation Bureau (CIU) is responsible for implementing the national strategies in combating computer crimes in Taiwan. CIU investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts, for instance the G-8 24/7 Computer Crime Network.

Some of the challenges faced by law enforcement on the international front include: harmonization of countries' criminal laws; locating and identifying perpetrators across borders; and securing electronic evidence of their crimes so that they may be brought to justice. Complex jurisdictional issues arise at each step. The Ministry of Justice is attending many anti-cybercrime international organizations and working with foreign governments through many channels to address global threats related to computer crime.

Cybercrime greatly affects individuals, businesses, and national security due to the pervasiveness of the Internet. We believe that different countries should work together and use legal, organizational, and technological approaches to combat cybercrime, to reduce the damage to critical infrastructures, and to protect the Internet from being abused.