



Global Business Dialogue on Electronic Commerce

GBDe 2006 Issue Group

**Cyber Security
“Threats and Countermeasures”**

*Issue Chair: Buheita Fujiwara, Chairman, Information-technology
Promotion Agency (IPA), Japan*

1. Overview

Cyber security is expanding its scope within the cyber and real economy. Cyber threats continue to escalate in variation and frequency. Efforts to fight cyber threats have involved a growing number of participants including governments, non-government public sectors, non-profit organizations and private organizations. Activities vary from legislation, public-private cooperation, commercial services and offerings as well as civil voluntary networking. International organizations provide treaties, recommendations and guidelines.

This report gives an overview of some of those activities and efforts, with references reported by some of the survey participants. Based on findings of the case studies, some recommendations are provided to make a better and safer cyber space.

2. Trends of Emerging Threats

Every country within the GBDe survey experiences some sort of threats. Typically, they are categorized into malicious codes, network attacks and network abuses. Malicious codes include computer viruses, worms, Trojan horses, spyware, key loggers, and BOTs. Network attacks typically include intrusions, DoS (Denial of Service) attacks and web defacement. Network abuse includes SPAM, phishing, pharming and network-related forgery.

There are two cases of attacking vulnerabilities. Software developers (e.g. Microsoft) release security updates to patch vulnerabilities for users. An attacker, then, analyzes this vulnerability and develops malicious programs to attack servers or client PCs which are

not yet updated. Usually, the period between the release of security update and the appearance of such attack is more than a month. However, recently, it is gradually becoming shorter and there are many examples with a very brief lead time such as a few days.

The other case is called the “Zero-day attack”. An attacker finds a new vulnerability and attacks it before the security update has been released. Such “Zero-day attacks” have been observed many times recently. Information on new vulnerabilities is not disclosed at the time of attack and hence the measure to rectify such vulnerability is not available. The cyber world faces an ever larger danger of software vulnerabilities.

The other point to be observed is monetary damages. Computer attacks are used to disturb the normal usage of computers, networks and data, and compromised web sites are used to send political messages or for propagation purposes. BOT net sometimes causes DoS attacks which result in network choking. Websites are sometimes compromised to show political messages or geopolitical harassment.

Now, offenders work to get real money. Last year the US experienced theft of credit card information in millions. In Japan a man sent spyware with a disguised complaint e-mail to a mail-order house to successfully get the customers’ credit numbers. Offenders attack any place where individual information could be available. Tools to intrude can be easily obtained from the Internet, and they are good at inventing social engineering and fraud methods. Threats are next to an innocent citizen’s door.

3. Statistics on Threats

Malaysian incident reporting includes “Monthly Abuse Statistics”, “Quarterly Summary of Incidents reported to NISER¹” and “Yearly Report”. Taiwan has an “Intrusion Alert and Advisory for Government Agencies”. IPA (Information-technology Promotion Agency of Japan) provides monthly and annual computer virus and malicious access statistics, associated with warnings and recommendations. US-CERT² publishes monthly bulletin handling vulnerability information. It also provides quarterly report on incidents. These are not specifically statistics on viruses and incidents. Virus statistics are typically provided monthly by anti-virus software vendors. Incident statistics come out from security information services providers.

The other statistical information is network monitoring reports. The IPA and a few other Japanese agencies including the National Police Agency periodically announce findings from network monitoring. Several private players, typically, security information service providers offer network monitoring information and early warning services as a commercial service.

¹ NISER: National ICT Security and emergency Response Centre, Ministry of Science, Technology and Innovation, Malaysia

² US-CERT: United States - Computer Emergency Response Team

4. Countermeasure Efforts against Threats

A type of Public-Private Partnership (PPP) to counter online security threats is active in Taiwan. Taiwan has also established a National CERT called ICST (Information & Communication Security Technology Center), which plays a key role in various activities to fight against Threats.

ICST has formed a network of 13,000 government officials to share and distribute computer emergency alerts and advisory information. ICST has also established a National Security Operation Center (NSOC) and this serves as a key organization in the Security Incident Data Exchange (SIDE_x) consisting of government Security Operation Centers (SOCs) and commercial managed security services providers. ICST is also active in training and education, including “Cyber Security Drills,” e-learning curriculums and CISSP training to the Government.

While serving mainly government sectors, ICST collaborates with private sectors in terms of SOC, early warning information sharing and security education.

In Malaysia, the National ICT Security and Emergency Response Centre (NISER) has been formed by the Malaysian Government to support the nation’s cyber security initiatives. Through collaborations between private and public sector organizations, NISER continuously identifies possible gaps that could be detrimental to national cyber security. MyCERT, a division under NISER is a national CERT for Malaysia that provides incident response services. They have established a National Cyber Early Warning Centre that provides monitoring and detection of potential cyber threats in Malaysia. For information sharing, they have successfully organized ICT Security forums, conferences and exhibitions. NISER, in collaboration with (ISC)², provides CISSP education and examinations. NISER is also active in cooperation with APCERT and other neighboring countries in combating cyber threats.

In Japan, various public and private entities work jointly and separately. The IPA and NICT (National Institute of Information and Communication Technology) together with AIST (National Institute of Advanced Industrial Science Technology) are the major government-sponsored agencies. All of these agencies are active in ICT security research and development. The IPA is responsible for the IT Engineers Examination, which is the largest examination in Japan.

Besides these government agencies, JIPDEC (Japan Information Processing Development Corporation) is active as the operator of ISMS certification and Privacy Mark authorization. Various industry associations, including JNSA (Japan Network Security Association), JASA (Japan Association of Security Audit) and NRA (Network Risk Management Association) are actively promoting network security and security management.

The IPA and JPCERT/CC jointly operates JVN (Japan Vendor Status Note), which is a website to share software vulnerabilities and solution information as a part of vulnerability information handling and coordination effort. (ISC)² Japan collaborates with JNSA to promote CISSP.

As seen above, and can be observed from the case of US-CERT and NISCC of UK, there is a distinctive commitment from the Government to information and network security. This indicates that cyber security deeply relates to national and social security. It also affects industry and consumers. Thus, the private sector is also active. An important and interesting point is that the public and private sectors work together in many countries. This is a natural tendency because cyber security is seamless over public and private entities.

5. Cyber-specific Laws against Threats

Cyber specific laws fall into three categories; enabling, prohibition and investigation.

Enabling typically gives legal effect to electronic documents and storage. For example, digital signatures can legally work as real signatures only when legislation provides such judicial capability. Evidence for tax or other purposes can be effective when a specific law defines electronic exchange and storage to be sufficient as evidence. The Digital Signature Act 1997 of Malaysia is a typical example.

Prohibition typically prohibits and punishes computer related crimes. In several countries, electronic data destruction cannot be criminalized under the general law, because it does not destroy any physical matter. Similarly, intrusion itself does not constitute a crime as it does no physical harm. Thus, a specific law is required. The Unauthorized Access Prohibition Law of Japan is a typical example of this type of law. The Computer Crimes Act 1997 of Malaysia is another example. These are the most typical law enforcement against threats.

For investigation purposes Internet services providers are typically required to reserve communication logs for a certain period of time and submit such records to national investigative agencies. As communication services providers are prohibited from divulging communications secrets, specific legislation is required to give exemption. Eavesdropping and network monitoring for specific communication also should be allowed under a jury court's order judged in line with a law allowing special investigation. The Communications Protection and Surveillance Act of Taiwan is a typical example of this type of legislation. These types of laws are prepared to indirectly fight against threats.

6. Non-cyber-specific Laws and Enforcement against Threats

A typical example of non-cyber-specific laws against threats would be the specific articles of penal laws. Penal laws usually handle only material crimes and damages. As

cybercrimes often destroy no physical material but electronic data, no physical damage is generated. However, economically, certain damage may occur.

The Malaysian Penal Code provides such effect with reference to Computer Crimes Act 1997. Article 234-2 of the Japanese Penal Code is another example. Computer operation disturbance itself constitutes a crime even when there is no physical damage. Criminal Code, Chapter 36 of Taiwan is also a similar example.

Besides specific cybercrime legislation, personal data or privacy protection laws also provide some protection. This does not necessarily relate to cyber threats, but cybercrime can often infringe privacy information. Therefore, privacy protection can also be deemed as non-cyber-specific law against threats.

7. Non-Government Regulations or Collaboration to Control Threats

Not many activities other than CSIRT collaboration were reported. Some Internet service providers in Japan control SPAM mail to protect their service bandwidth. SPAM mail control requires mail content monitoring, and it might constitute an infringement of the secrecy obligation of carriers. Yet, protection of network from abuse is a very important issue which every player should seriously think over.

8. Criminalization in Relation to the Cybercrime Convention

The Cybercrime Convention of the Council of Europe calls for eight offenses to be criminalized:

1. Illegal interception
2. Data interference
3. System interference
4. Misuse of devices
5. Computer-related forgery
6. Computer-related fraud
7. Offenses related to child pornography, and
8. Offenses related to infringement of copyright and related rights.

Japan and Malaysia provide legislation for all of these offenses. These offenses are typically regulated by the Criminal Code or cyber-specific laws such as the Communications and Multimedia Act 1988 and Cyber Crime Act 1997 of Malaysia.

The Convention also calls for legislation of six legal procedures:

1. Preservation of computer data
2. Preservation and partial disclosure of traffic data
3. Production order
4. Search and seizure of stored computer data
5. Real-time collection of traffic data, and

6. Interception of content data.

Japan legally provides all of the six procedures. Malaysia is the same, yet some are not officially provided, or on the way.

9. OECD Initiatives to Fight SPAM

The trouble with SPAM grows day by day. On April 19, 2006, the OECD announced a recommendation which urges government and industry to fight against SPAM in international harmonization and public-private partnership. Japan has some laws to restrict SPAM. Efforts from tool vendors and communication carriers take place, but are not really effective. Malaysia reported a detailed domestic and international collaboration to fight SPAM. SPAM continues to be an ever expanding headache among the Internet citizens.

10. Other Civil and Industrial Efforts

Malaysia provided information about a cyber early warning initiative, CEWS (Cyber Early Warning Service), which monitors and detects cyber attacks in the early stage. Malaysia has also held international CERT Workshops and Cryptology Conferences. For information sharing amongst the members, Special Interest Groups and a Mailing List have been established.

Japan reported early warning-related civil activities and Telecom-ISAC (Information Sharing and Analysis Center), and other civil collaborations aimed to share and distribute information among member firms and industry stake holders.

11. Overall View

Countries/economies participating in the survey reported active efforts against threats from both governmental side and private sector side. The public sector side includes legislation and administrative initiatives while the private sector side contains various activities. The most typical activity is CSIRT, and CSIRT has established an international collaboration network. Cyber space is borderless, so the efforts against cyber threats should be international. The social framework, though, is based on each country. Thus, governmental efforts including legislation, administrative actions and national funding are important.

12. Recommendations

Based on findings and observations made following the 2006 survey and related study by the Cyber Security Issue Group, the GBDe would like to give the following recommendations for cyber space participants to fight against threats.

A. Better Awareness of Users

Individual users do not have enough information about the danger of cyber threats. As cyber attacks tend to aim at money, they face a bigger risk of fraud and financial damages. Many Internet users are easily lured by unknown mails and web site buttons, falling victim to spyware and phishing.

Education of users is most important. Japan's METI, the IPA, and Chamber of Commerce run security seminars for corporate users every year all over the country. METI and JNSA also offer Internet literacy classes for citizens in towns across Japan to lecture about the danger in a simple, easy and friendly manner (e.g. using comics and short videos).

This is a typical area where public-private collaboration can work well. It is recommended that every country should have such educational program or activities to improve civil awareness of cyber threats.

B. Law Enforcement

The GBDe has observed that many countries now have legislation against cybercrime. Legislation is not a simple solution. There are areas of conflicts involving human rights and communication secrecy, and a trade off of between deregulation and industrial order.

The other difficulty is that cybercrime can take place regardless of borders, but legislations and jurisdictions are based on a nation-by-nation framework. So, international collaboration and coordination are very important. If an international, seamless restriction and regulation network could be established, it would provide a great boost to efforts to suppress cyber threats.

Information technology evolves day-by-day. Cybercrime technology is also constantly evolving. Hackers invent IT and social engineering methods to commit cybercrime. The important thing to prevent cybercrime is, therefore, to cover any security holes. It is also necessary to ensure better quality through improved software engineering development. An early warning partnership to eliminate vulnerabilities is another potential area of major benefit. The final point is to fill the legislation gaps and holes among countries. Do not create a hacker haven.

C. Damage Control

Completely exterminating cybercrime is impossible, just as real crime cannot be completely suppressed. The next best alternative is to prepare for unexpected attacks and damages.

Prevention is one way. Precautions, protections, detections and preventions should be properly implemented. Tools and services are available. Employ appropriate and effective prevention measures.

Mitigation is the next step. In order to minimize the impact of attacks, it is important to prepare for incidents. Measures to limit the extent of damage include the creation of a

backup to enable rapid recovery. This helps businesses resume with limited loss and system down time. Business continuity planning should also include damage mitigation strategies.

D. Collaborative Fight against Threats

CSIRTs play a key role in the defense against cyber threats in many countries and regions. These include both government and non-governmental CSIRTs. Although they have formed an effective international network, the GBDe would like to see collaboration expand between participants. What the international community and respective national governments should do is to reinforce support for CSIRTs so that they can be more active.