Implementing Information Security to Protect Individuals' Privacy

The development of new technology is bound to have both positive and negative effects. However, when a new technology is first introduced, it is common for insufficient attention to be paid to its negative aspects, either because there has not been time to accumulate sufficient experience in using it or because users are blinded by the potential benefits. It is only later, when the technology begins to be abused, that people wake up to the potential dangers. The evolution of computers and the Internet is a classic example of this phenomenon. While the rapid development of information technology has helped to stimulate the flow of information in every corner of society, cyberspace has also become the setting for a wide range of criminal activities. In many cases, countries' existing legal and regulatory frameworks have proved inadequate to cope with the threat posed by the various forms of unauthorized access. A variety of forms of cyber-crime have developed, including denial-of-service attacks, unauthorized accessing of databases, phishing, identity theft and online fraud or intimidation. Cyber-crime may involve making unauthorized use of individuals' personal information, stealing companies' confidential business information or selling state secrets; these new types of crime thus affect every level of society. The effects can be catastrophic, hence the growing importance is now being attached to information security, including both the establishment of effective management mechanisms to prevent cyber-crime from occurring in the first place and the development of the capabilities needed to detect such crime when it occurs. Recognizing the need to plug the gaps in the existing legal and regulatory framework in the face of cyber-crime, countries all over the world are working on the formulation of new legislation, and Taiwan is no exception. The following sections will discuss the key developments in the laws and regulations governing information security in Taiwan in recent years.

I. The Convention on Cyber-crime and Chapter 36 of Taiwan’s Criminal Code (offences relating to the abuse of computers)

Today, governments throughout the world are formulating measures to combat criminal activity that makes use of the Internet (cyber-crime). In many cases these measures are based on the Convention on Cyber-crime announced by the European Commission on November 23, 2001, and which came into effect on July 1, 2004. This convention is the first international agreement to be established specifically to combat cyber-crime. Its contents include discussion of the various types of cyber-crime, regulations governing the obtaining of electronic evidence, provisions for mutual assistance between nations in judicial matters with respect to cyber-crime and measures to encourage multilateral collaboration. The European Commission asked all signatory nations to revise their own national laws so that they conform to the provisions of the Convention, with the aim of establishing a unified international framework for combating cyber-crime.

Responding to the international trend towards the enactment of legislation to fight cyber-crime and to eliminate any loopholes in Taiwanese law that might result in Taiwan becoming a haven for cyber-criminals, on June 25, 2003 the Taiwanese government added a new chapter, Chapter 36 (Offences Relating to the abuse of Computers) to Taiwan's Criminal Code. It contains six articles covering four types of crime: unauthorized access (Article 358), the unauthorized acquisition, deletion or titleeration of electromagnetic records (Article 359), unauthorized use of or interference with a computer system (Article 360) and creating computer programs specifically for the perpetration of a crime (Article 362). Article 361 specifies that more severe punishment should be imposed in the case of violations carried out against the computers or other equipment of a public service organization, and Article 363 states that the provisions of Articles 358–360 shall apply only after prosecution is instituted upon complaint. These new articles provide a clear legal basis for the punishment of common types of cyber-crime such as unauthorized access by hackers, the spreading of computer viruses and the use of Trojan horse programs. In formulating these articles, reference was made to the categorization of cyber-crimes used in the Convention on Cyber-crime and to the suggestions for revision of national laws put forward there. Article 36 is thus in broad conformity with current international practice in this regard and can be expected to achieve significant results in terms of combating cyber-crime.

II. The authority of law enforcement to get evidence and ISPs liability

In its discussion of the securing of electromagnetic records by law enforcement agencies, the Convention on Cyber-crime notes that such securing of records falls into two broad categories: immediate access and non-immediate access. Immediate access includes the monitoring of communications by law enforcement agencies, non-immediate access relates mainly to the data retention obligations imposed on Internet Service Providers (ISPs).

As regards the regulatory framework for the monitoring of communications, Communications Protection and Surveillance Act came into effect in Taiwan on July 16, 1999. According to its provisions, monitoring of communications may only be implemented when it is deemed necessary to protect national security or to maintain social order. Warrants for such surveillance may only be issued if the content of the communications is related to a threat to national security or to the maintenance of social order. Furthermore, the crime in question must be a serious one. In principle, the period for which surveillance is implemented should not exceed 30 days. These restrictions reflect the government’s determination to ensure that citizens' right to privacy is protected.

While the Internet is an environment conducive to the maintenance of anonymity, electromagnetic records are easy to erase. Effective investigation of cyber-crime requires automatic recording of communications by the equipment used to transmit the messages, that is to say, it requires the retention of historic data. As regards the extent to which companies are required to collaborate with law enforcement agencies and the conditions applying to the making available of electromagnetic records, these issues relate to the public's right to privacy, and the law in this area needs to be very clear and precise. For the most part, data retention obligations are laid down in Taiwan’s Telecommunications Act. In Taiwan ISPs are classed as "Type II Telecommunications Operators". Article 27 of the Administrative Regulations on Type II Telecommunications Businesses stipulates that Type II telecommunications operators may be required to confirm the existence of, and provide the contents of, customers' communications for the purpose of investigation or collection of evidence upon request in accordance with the requirements of the law. ISPs are required to retain, for a period of between 1 and 6 months, data relating to the account number of subscribers, the times and dates of communications, the times at which subscribers logged on and off, free e-mail accounts, the IP addresses

used when applying for Web space and the time and date when such applications were made, the IP address used to make postings on message boards and newsgroups, the time and date when such postings were made and subscribers' e-mail communications records. If a Type II telecommunications operator violates these provisions, he may be fined between NT$200,000 and NT$1 million and be required to remedy the situation within a specified time limit in accordance with Paragraph 2 of Article 64 of the Telecommunications Law. If he fails to remedy the situation within the specified time limit, his license may be revoked.

III. The Legal Framework for Personal Data Protection

titlehough, as outlined above, some revisions have already been made to the legal framework governing information security, there are still many areas which need to be reviewed. One of the most important is the protection of personal information. Following the explosive growth of the Internet, customer-related information is being processed by computers on a large scale in many different industries. With so many companies collaborating with other firms or adopting new marketing methods, the value and importance of personal information is being reassessed. The dramatic increase in the number of online scams in Taiwan in recent years has made the protection of privacy a focus of attention. The existing Computer-processed Personal Data Protection Law, drawn up to target specific industries, does not really provide adequate protection.

A new Personal Data Protection Act, drawn up with reference to the European Union's Directive (95/46/EC) on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data and the personal information protection legislation adopted in the USA and Japan, has already been submitted to the Legislative Yuan for deliberation. The key differences between this new Act and the existing Computer-processed Personal Data Protection Law are as follows. Protection is no longer industry-specific, it now applies to both natural and juristic persons and to both public and private agencies. The scope of protection has been expanded to include hard copies of documents containing personal information, and five new types of "sensitive information" – information relating to criminal records, medical examinations, medical records, sexual history and genetic information – have been added. Special restrictions apply to the collection and processing of these types of data. The Personal Data Protection Act also imposes stricter requirements on public and private agencies with regard to the protection of individuals' personal data. For example, agencies must formulate personal data protection plans and measures for dealing with personal data once those data are no longer needed for business purposes. If an agency discovers that an individual's personal data have been stolen, leaked, titleered or violated in any way, they are required to notify by telephone or letter the agency responsible for notifying the individual concerned as soon as possible. If these provisions are violated, the agency's responsible person will be liable for administrative punishment. The new Act also gives regulatory authorities greater powers to undertaking auditing in this area, makes provision for class action suits and increases the amount of compensation to be paid to victims. It is expected that these mechanisms will help boost awareness of the importance of information security in all sectors, thereby helping to ensure better protection for the public's personal information.

IV. Management of Unsolicited Commercial E-Mail

The widespread utilization of e-mail has created a brand new marketing channel, so that e-mail can fairly be described as one of the most important "killer applications" to which the Internet has given rise. Today, spamming is causing serious problems for both e-mail users and ISPs. E-mail users are concerned about their privacy being violated and about having their e-mail box stuffed full of junk e-mail. Spamming also ties up bandwidth which could be used for other purposes, and Distributed Denial of Service Attacks (DDOS) can make it difficult for ISPs to provide normal service to their customers. Governments throughout the world have begun to consider whether anti-spamming legislation may be necessary. In Taiwan draft legislation of this type has already been submitted to the Legislative Yuan.

Taiwan's Anti-SPAM Act was drawn up with reference to the USA's CAN-SPAM Act of 2003, Japan's Law on Regulation of Transmission of Specified Electronic Mail, Australia's SPAM Act and the UK's Privacy and Electronic Communications (EC Directive) Regulations 2003. The draft SPAM Act contains 13 articles, with an emphasis on self-regulation, technology filtering and provision for seeking compensation through civil action. The Act provides for the use of an "opt-out" mechanism to regulate the behavior of e-mail senders, with the following obligations to be imposed on them. (1) The sender must specify in the "Subject" field of the e-mail whether it is a "business communication" or "advertising" to facilitate filtering by ISPs and to make clear to the recipient what type it is. (2) The sender must provide accurate information, including header, information on the sender's identity and the sender's e-mail address. (3) E-mails may not be sent if the sender knows or could be expected to know that the intended recipient has already expressed a wish not to receive e-mail from this source. E-mails may also not be sent if the sender knows or could be expected to know that the information in the "Subject" field is inaccurate or misleading. If the sender continues to send e-mails after the recipient has expressed a clear wish not to receive any more from the sender or if the sender falsifies the "Subject" or header information, then the sender may be required to pay compensation to the recipient at a rate of NT$500–2,000 per person per e-mail. With regard to the widespread practice whereby companies or advertising agencies commission third parties to send junk e-mail on their behalf, in cases where the commissioning party knows or could be expected to know that e-mail is being sent in violation of the above regulations, the commissioning party shall be held jointly liable with the party sending the e-mail. Through the implementation of this new law, the government hopes to establish a first-class Internet environment in Taiwan, putting an end to the current situation whereby large numbers of businesses are engaged in spamming.

V. Conclusions

Security is the biggest single factor affecting the implementation of e-government initiatives, e-business application adoption and Internet user confidence. Most people associate information security only with the purchasing of security hardware or software and the setting up of firewalls. While these products can indeed help to make the online environment more secure, Internet users should not allow themselves to be lulled into thinking that buying these products will in and of itself be sufficient to ensure security. "Security" is a fluid concept. Over time, the level of security that even a high-end product can provide will deteriorate; the fact that your system is secure now does not guarantee that it will remain secure in the future. Evidence that this is true is provided by the damage that is constantly being caused by viruses, by the need to

constantly update security products and by the shift in emphasis away from virus prevention and firewalls towards preventing "backdoor" attacks and towards proactive intrusion detection. Furthermore, the information security risks that companies and organizations have to deal with are not limited to external threats; poor internal management may result in employees selling or leaking customer data or other company data, which can cause serious damage to the organization.

Examination of information security theory and practice in Taiwan and overseas suggests that the establishment of effective information security measures embraces four main areas: the detection of cyber-crime, development of new information security technologies and formulation of standards, education and management of computer users and regulatory and policy issues. The most important of these is the education and management of computer users. Detection of cyber-crime is the next most important, while development of new technologies and standard setting and the regulatory and policy aspects play a supporting role. To create a genuinely secure online environment, attention must be paid to all of these. Today governments throughout the world are formulating new legislation to plug the gaps in the regulatory framework governing the online environment. Given the need to let the market mechanism operate freely and to refrain from measures that might retard industrial development, government interference in the Internet, with the exception of crime prevention activity, has generally been viewed as a last resort. Currently the government in Taiwan is still focusing mainly on self-regulation by Internet service providers and other types of business enterprise, and the government's role is still largely confined to formulating standards and assisting with the development of new security products. The area on which both the government and the private sector will need to concentrate in the future is educating and ensuring effective management of computer users.

Release : 2013/04

Tag