I-WAYS, Digest of Electronic Commerce Policy and Regulation 28 (2005) 119–125
IOS Press

In Brief

Corporate Information Security Plan for Japan

For several years the Japan Business Federation (Keidanren) has been exploring concerns of the Japanese business community about the "roles that companies, government and individuals must play in order to realize a secure and safe Internet society." On March 15, 2005 a report entitled Policy Proposal on Corporate Information Security in Japan was distributed. This follows a report in May 2004 revising Keidanren's Corporate Behavior Charter that stresses "the information society has moved from being a technical issue to one of corporate governance, social responsibility and corporate legal compliance." The Charter sets forth ten principles that Keidanren member companies "should observe in establishing internal procedures: by the development and provision of socially beneficial goods and services in a safe and responsible manner (companies) shall strive to earn the confidence of their consumers and customers while taking necessary measures to protect personal data and customer related information."

The report characterizes "information security as a business challenge – from defensive information security to offensive information security." It points out that until recently, corporate information security measures have been optional efforts for sustaining business and gaining the trust of customers. However, with the amendment of the Personal Information Protection Act and the unfair Competition prevention Law, information security is now a matter of compliance and in contracts between companies there are increasing number of cases in which third-party certification is sought with regard to information security.

There are several issues identified for companies relating to information security measures. The following are excerpts from the report:

1. For companies serious about making information security a priority, top management must understand the importance of information security, and ensure that measures are accordingly implemented top-down. Companies that have insufficient security measures face difficulties in gaining the cooperation of the entire company regarding the promotion of data protection measures. Even if the manager in charge of information security at the company tries to move forward with some measures, many managers view information security as a burdensome cost, because it is difficult to see the cost-benefit performance of an investment in information security. In the absence of leadership by senior management, it is difficult to create a mindset in which information security measures are actively promoted. Furthermore, in moving forward with information security measures, long-standing business practices must be changed which typically prompts resistance from people other than managers.
2. It is necessary for companies to strike a "rational level" of information security. Many companies that are aware of the importance of data protection are working to strike a "rational level" of information security that balances the management of information and the utilization of information. Some companies aim for 100% security, which is impossible to achieve, and as a result of implementing extreme security measures, have actually disrupted their business activities. So-called "eco-friendly companies" are praised in the market. But measures taken by companies with regard to information security are by their very nature difficult to publicize and there is still not a measurement index in the market that rewards security-conscious companies. As such, there are concerns that even if information security measures are implemented seriously, they will not be highly evaluated in the market despite their cost, and as a result the short-term competitiveness of companies that seriously implement information security measures will decline.
3. Cooperative efforts for information management are needed in terms of compliance. Many companies are moving forward with all-out efforts to

ISSN 1084-4678/05/$17.00

appropriately handle the information they possess and education their employees in accordance with the provisions of the law. Regardless of the extent to which companies develop structures, it is impossible to absolutely prevent employees from taking actions with dishonest intentions. In addition, it is necessary for companies and governments to cooperatively develop those measures in cases of illegal employees disclosures of private information. Various ministries and agencies have formulated guidelines for the areas under their jurisdiction regarding the handling of personal information, but the regulations imposed on companies are different for each ministry and agency, causing confusion at workplaces that handle personal information.

4. Promotion of information security measures by companies and governments. With regard to efforts by companies, they should voluntary implement all conceivable measures to the utmost extent possible. The basis of information security lies in focusing on vulnerabilities in companies and decreasing risk, by reducing those vulnerabilities. Keidanren calls on members to utilize the Corporate Behavior Charter and to consider the inclusion of the following specific efforts:

   a. raising awareness regarding information security within companies, starting with top management;
   b. top management should take the initiative and make efforts with regard to information security measures;
   c. the Chief Information Officer (CIO) or the Chief Security Officer (CIO) is the responsible manager; and
   d. existing standards such as Information Security Management System (ISMS) should be utilized in implementing information security measures, including formulating security policies, carrying out external auditing, developing governance, and implementing security technology.

   Currently efforts by governments at both central and local levels, are working to raise the level if information security in Japan as a whole and in addition to existing measures, however it is necessary to think about information security measures for the entire country, including companies. When governments plan and design policies, they set objectives for what should be accomplished at what dates and steps to take. In addition to examining compartmentalized information security policies among ministries and agencies, strategies for Japan as a whole are needed so the public will embrace the necessary changes.
5. Effective measures for preventing leaks of personal information by implementing the Personal Information Protection Act, requires that companies select information that should be protected from leaks including personal information based on provisions of the law, and develop a system for protecting this information. Nonetheless, it is impossible to completely prevent incidents such as leakages, even if organizational and technical management systems are strengthened.

Digital Broadband Content – Changing Value Chains and Business Models

"Rapid high-speed development and innovative use have resulted in convergence in the capacities and potential use of fixed and mobile platforms with experiments in business models for content delivery and use." This is a conclusion of the OECD Working Party on the Information Society. The panel had as its mission to analyze and discuss changing digital content value chains and business models, and identify new challenges and issues facing the development and delivery of digital content. The report, Digital Broadband Content (DSTI/ICCP/IE(2004)15/FINAL) resulted from a June 2004 session, presents highlights and findings.

The panel received presentations from governments of the United Kingdom, Japan, Norway, the US Federal Communications Commission (FCC), South Korea and Italy. Officials from these governments presented details on the changing environments in the digital world from policy and regulatory perspectives.

The following are excerpts from an overview of digital content and value chain developments presented in the report:

Recent developments: Central concepts in relation to content are mobility and sharing. Non-commercial peer-to-peer networks have experienced fast take-up indicating that there is demand for new commercial content delivery services and business models based on

easy, deep access and subscription models. The music industry has already developed successful business models.

Issues identified: Relations between network service providers (fixed and mobile), technology suppliers (e.g. handsets) and content providers are changing and complex new market structures and business relationships are evolving. Often the challenge is to move from a model based on advertising to a model based on paid subscriptions/content. Positive revenue feedback cycles are generated when growing subscriber numbers foster the development of online content and services that in turn draw more subscribers.

Outlook and issues: Continued turbulence, but the first workable business models are in operation and generate substantial revenues. Broadband video services and "Triple-Play" (voice, broadband and standard or on-demand audiovisual services) from ISPs will provide further growth. Industry players are continuing to experiment and new business partners result.

The OECD Panel reviewed several generic themes. These are:

- Network convergence and rapid diffusion of high-speed broadband has shifted attention towards broadband content and applications (new demand for the digital economy) that promise new business opportunities, growth and employment. The potential for digital content growth is very high and growth is only just beginning. Technologies to assure the diffusion of content and content products are increasingly R&D intensive (faster networks, new platforms, software intensive products, virtual reality applications, data-base management, etc.)
- Demand for content from consumers and intermediaries exploiting the potential of multiple content delivery channels is extending and supplanting infrastructure as a major driver.
- Disruptive technologies and broadband in particular are challenging established business models while creating important development opportunities in all three sectors. Mobile content and applications received particular attention and are potentially major drivers of mobile telecommunications service and content industry revenues in OECD countries.
- The relationships between content originators and final users are changing, intermediaries are being created or replaced, and attitudes to content ownership and acquisition are changing. However, complete disintermediation and direct contact between content creators and content users has not so far developed to a significant extent in the three sectors.

Cyber Security Solutions for VoIP

Increasing broad adoption of IP-enabled technologies, such as VoIP, calls for heightened focus on protecting the security, integrity and reliability of the Internet, according to the Cyber Security Industry Alliance (CSIA). The Washington-based organization (www.csialliance.org) has released a report that recommends Congress consider cyber security issues facing VoIP as it considers revising the Telecommunications Act of 1996.

The Report finds that the same qualities that make VoIP such a valuable new option for mass-market voice communications also can lead to quality of service and performance issues including denial of service attacks, Spam over IP Telephony (SPIT), session eavesdropping and voicemail hijacking. The report concludes that adding an extra layer of security infrastructure can help resolve some of these issues, but not all of them. Since voice communication is a key enabler of critical government services operated by national security and emergency preparedness providers, a VoIP cyber attack could lead to serious consequences, such as loss of public access to critical emergency services like 911.

"While the promise of IP telephony is economical for many organizations, cyber security issues cannot be ignored," said Paul Kurtz, executive director of CSIA. "Because IP telephony depends solely on the Internet for operating, it is subject to all the same vulnerabilities that our corporate networks face. As Congress considers revisiting the Telecommunications Act of 1996, CSIA strongly recommends that the serious implications of VoIP cyber attacks be addressed since they can affect critical government services such as 911 and other emergency first responder services."

CSIA points out that as consumers, businesses and government make much more intensive use of the IP platform through voice applications, it is essential to address the resulting impact on national security, emergency preparedness and Internet fraud/criminal activity. This report demonstrates the potential for VoIP to provide another channel for exploiting vulnerabilities

in both our critical infrastructure and the IT-based economy. VoIP vulnerabilities also have the potential to act as entry points for attacks on the rest of the network, including non-VoIP applications, systems and infrastructures. Some potential fallout examples include:

- Crippling impacts on the operations of IT dependent critical infrastructures, including the potential knock out of banking, finance, chemical, electric power generation and distribution, oil and gas production and storage, emergency services, public health services, transportation systems, water supplies and more;
- Disablement of IT supporting critical infrastructures in these industries;
- Potential for weakening the national response capability as part of a blended cyber and physical attack;
- Loss of revenue for operation stoppages in call centers, order processing and shipping;
- Theft, erasure, or alteration of business and personal information; and
- Violations of privacy and confidentiality regulations, possibly resulting in civil and/or criminal penalties.

The organization believes that cyber security for VoIP is essential for the protection of the entire information technology ecosphere and asks that Congress consider several recommendations for securing VoIP technologies, including supporting research & development aimed at improving the security and reliability of VoIP as well as defining roles and responsibilities for agencies such as the Department of Homeland Security, the Federal Communications Commission and the Department of Defense.

UK Internet Telephone Service Providers Adopt Consumer Code of Practice

With more and more VoIP services launching every week, how do UK consumers know which services to trust? Is there someone they can complain to if they are not happy? Can they make emergency (999) calls from their VoIP phone? To help improve consumer information and awareness and to give consumers confidence that they are getting a service from a reputable provider with proper consumer protection in place the Internet Telephony Services Providers' Association (ITSPA) has launched a consumer Code of Practice (CoP). ITSPA Members who adhere to the Code of Practice (CoP) will have the right to display the ITSPA logo on their website. ITSPA hopes that consumers will come to recognize the logo as a badge of excellence for VoIP providers, giving them the confidence to try VoIP services from its members.

The ITSPA CoP is the fruit of many months of discussion and consultation. All ITSPA members providing services to consumers must abide by this Code and inform their customers of the differences between VoIP services and traditional telephony services. Consumers can trust the ITSPA logo to represent VoIP providers offering a high standard of consumer information awareness. Members of ITSPA claim "this is a world first, and vital to ensure the rapid uptake by the mass-market of this new generation of services." The ITSPA Council had stressed it plans to act efficiently in administering and enforcing the code. The UK Department of Trade and Industry and telecommunications regulator, Ofcom are reported to welcome the ITSPA code.

ITSPA was established with the following mission:

- The benefits of self-regulation to promote the growing VoIP sector;
- The need to foster a truly competitive and innovative market where VoIP providers can compete with existing telecoms providers on a level playing field;
- The facilitation of the provision of "naked DSL" (i.e. the provision of broadband access without needing to also pay for telephone line rental);
- Open, non-discriminatory access through all Broadband ISPs (i.e. ISPs should not block/hinder customers from using third party VoIP providers);
- The promotion of best efforts provision of access to emergency services and the provision of accurate information to the consumer about the level of access to emergency services available to them;
- Effective and competitively priced Local Loop Unbundling;
- The use of geographic numbers for VoIP providers;
- Efficient and competitively priced number portability (i.e. the ability to transfer/retain your phone number when you change service provider).

The ITSPA Secretariat can be contacted via email at secretariat@itpsa.org.uk. The ITSPA Code of Practice can be viewed at: http://www.itspa.org.uk/cop.htm.

US RFID Passport Plan Revised

Following criticism from computer security professionals and civil libertarians about the privacy risks posed by new RFID passports the US Government plans to begin issuing, a State Department official said recently that his office is reconsidering a privacy solution it rejected earlier that would help protect passport holders' data. The solution would require an RFID reader to provide a key or password before it could read data embedded on an RFID passport's chip. It would also encrypt data as it's transmitted from the chip to a reader so that no one could read the data if they intercepted it in transit. This would prevent skimming and eavesdropping by unauthorized persons.

Reading distance refers to the distance from which an RFID chip can be read. The new RFID passports, or e-passports, were designed with a contactless chip in the back cover, which allows officials to read electronic data on a passport from a distance, using an electronic reader. The distance depends on the design of the chip and the reader.

US officials had maintained that the passport chips to be used could be read from only 10 inches away. But at least one test showed that a reader could read a passport chip from 30 feet away. Because initially the US had decided not to encrypt data contained on passport chips, the chips exposed passport holders to privacy risks, such as skimming and eavesdropping. Skimming occurs when an intruder with a reading device in the vicinity of the passport holder surreptitiously reads the electronic information on the chip without the passport holder knowing. Eavesdropping is when an intruder intercepts data as it's being transmitted from the chip to an authorized reader.

The International Civil Aviation Organization, which created the international specifications for countries adopting RFID passports, designed specifications for a process called Basic Access Control (BAC). The data on a passport would be stored on an RFID chip in the passport's back folder, but the data would be locked and unavailable to any reader that doesn't know a secret key or password to unlock the data. To obtain the key, a passport officer would need to physically scan the machine-readable text that's printed on the passport page beneath the photo (this usually includes date of birth, passport number and expiration date). The reader would then hash the data to create a unique key that could be used to authenticate the reader and unlock the data on the RFID chip.

BAC prevents skimming because it doesn't allow remote readers to access data on the passport without the passport being physically opened and scanned through a reader. It also prevents eavesdropping since it would encrypt the communication channel that opens when the data is sent from the chip to the reader.

A State Department official noted this solution was originally rejected because the United States never planned to include more data on the RFID chip than what could be easily read simply by looking at the passport. That being the case, they believed that anti-skimming technology, such as metal fibers in the passport cover, would prevent anyone from surreptitiously reading a passport as long as it was closed. It was originally thought that the chip could not be read at a distance of more than 10 inches (when the passport was open) but now the Department finds that perhaps there are some more serious threats in the area of read ranges. The use of BAC gives additional protection when the book is actually open. The German Government and other members of the European Union had embraced BAC because they plan to write more data to the chip than just the written data that appears on the passport photo page. Many countries plan to include at least two fingerprints, digitized, in their passport chips.

Ubiquitous Gigabit Network Promoted in US

The United States should deploy widespread wired and wireless gigabit networks as a national priority, according to a white paper from the IEEE-USA Committee on Communications and Information Policy (CCIP). The paper urges that "our nation must act promptly to ensure that a new generation of broadband networks – of gigabit per second speed – is ubiquitous and available to all. Failure to act will relegate the US telecommunications infrastructure to an inferior competitive position and undermine the future of the US economy."

Digital data rates, or speeds, are typically expressed as megabits per second (Mbps) or gigabits per second (Gbps). A megabit is one million bits; a gigabit is one billion bits. Current broadband networks, such as DSL or cable modems, have an asymmetric speed of about 2 Mbps. Gigabit networks are capable of digital rates 50 to 5,000 times as fast, with equal upstream and downstream speed. Symmetric speed means information can be downloaded and uploaded at the same rate. With asymmetric systems, upstream speeds lag behind downstream delivery rates.

Omnipresent US gigabit networks, readily achievable by deploying optical fiber and high-speed wireless, would carry numerous benefits. These include providing the US economy with superior ability to compete globally; stimulating economic activity in digital home entertainment; enhancing online education and training; and facilitating health care remote diagnosis and consultation (telemedicine).

The Congress, the Executive Branch and private-sector initiatives could secure these benefits for the nation's global competitiveness and quality of life by adopting "principles leading to ubiquitous, symmetric gigabit availability as a national priority, according to the CCIP white paper (www.ieeeusa.org/volunteers/committees/ccip/docs/Gigabit-WP.pdf). Such principles include regulatory flexibility and encouragement of user-owned networks.

"The key fact of modern telecommunications is the convergence of voice, data, image and video into digital bit streams," said Dr. John Richardson, a former chief scientist at the National Telecommunications and Information Administration. "We need faster networks to carry these bit streams to users. Broadband speed and penetration in the United States are pitiful compared to levels in Japan and South Korea. This means that US prosperity is at risk because it depends, in large part, on fast and easy exchange of information."

IEEE-USA is an organizational unit of the IEEE. It was created in 1973 to advance the public good and promote the careers and public policy interests of the more than 220,000 technology professionals who are US members of the IEEE. The IEEE is the world's largest technical professional society. For more information, go to www.ieeeusa.org.

E-Government Advances in US Agencies

The US E-Government Act of 2002 is intended to promote better use of the Internet and other information technologies to improve government services for citizens, internal government operations and opportunities for citizen participation in government. Among other things, the act specifically requires the establishment of the Office of Electronic Government within the Office of Management and Budget (OMB) to oversee implementation of the act's provisions and mandates a number of specific actions, such as the establishment of interagency committees, completion of several studies, submission of reports with recommendations, issuance of a variety of guidance documents, establishment of new policies and initiation of pilot projects. Further, the act requires federal agencies to take a number of actions, such as conducting privacy impact assessments, providing public access to agency information, and allowing for electronic access to rulemaking proceedings. OMB has linked several of the act's provisions to ongoing e-government initiatives that it has sponsored.

In a recent report on Electronic Government, the US Government Accounting Office (GAO) indicates that "in most cases OMB and federal agencies have taken positive steps toward implementing the provisions of Titles I and II of the E-Gov Act." This and other GAO documents are available from www.gao.gov. According to the GAO report: "OMB established the Office of E-Government as the office's Administrator in 2003, published guidance to federal agencies have taken action to address the act's requirements within stipulated time frames. For example, OMB established the Interagency Committee on Government Information in June 2003, within the deadline prescribed in the act. The committee is to develop recommendations on the categorization of government information and public access to electronic information. In all but one case, OMB and agencies have taken action to implement the act. For example, the federal courts have established informational Web sites in advance of the April 2005 deadline specified in the act, and court officials are taking steps to ensure that the Web sites fully meet the criteria stipulated by the act."

"Similarly, in most cases where deadlines are not specified, OMB and federal agencies have either fully implemented the provisions or demonstrated positive action toward implementation. For example, in May

2003, the E-government Administrator issues a memorandum detailing procedures for requesting funds from the E-Government Fund, although the act did not specify a deadline for this action.

Although the government has made progress in implementing the act, the act's requirements have not always been fully addressed. Specifically, OMB has not:

- ensured that a study on using ITW to enhance crisis preparedness and response has been conducted that addresses the content specifically specified in the act,
- established a required program to encourage contractor innovation and excellence in facilitating the development and enhancement of electronic government services and processes, or
- ensured the development and maintenance of a required repository and Web site of information about research and development funded by the federal government.

Further, GSA has not contracted with the National Academy of Science (NAS) to conduct a required study on disparities in Internet access for online government services."

To ensure the successful implementation of the E-Government Act and achievement of its goals, GAO is making a number of additional recommendations to the Administrator of E-Government in OMB.