View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by The University of North Carolina at Greensboro

Japan's Changing Cybersecurity Landscape

By: Nir Kshetri

Kshetri, N. (2014). Japan's changing cyber security landscape, *Computer, 47(1)*, 83–86. doi: 10.1109/MC.2014.17

Made available courtesy of Institute of Electrical and Electronics Engineers (IEEE): http://dx.doi.org/10.1109/MC.2014.17

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works

*****© IEEE. Reprinted with permission. No further reproduction is authorized without written permission from IEEE Computer Society. This version of the document is not the version of record. Figures and/or pictures may be missing from this format of the document. *****

Abstract:

Japan's cybersecurity efforts have been lacking compared to other advanced economies, but the country is now taking more aggressive steps to address this deficiency.

Keywords: Japan | cybersecurity | cyberdefense

Article:

As late as 2012, Japan hadn't officially acknowledged cyberattacks as a national security threat (http://tinyurl.com/k4rgawn). A British official involved in cybersecurity recently went so far as to assert that Japan has "zero capability" and lacks "situational awareness" (http://tinyurl.com/kmhghy7). For instance, in 2011, hackers stole online credentials of Lower House Diet members and their secretaries, giving the perpetrators access to emails and documents possessed by the 480 lawmakers and other personnel (http://tinyurl.com/lr8rg6r). Reportedly only 45 percent of lawmakers changed their passwords following the attacks.

Due primarily to this and other high-profile cyberattacks as well as internal and external pressures, Japan has revised its cybersecurity strategies. Policymakers realize that the country's data privacy related regulations have acted as a barrier to cloud computing and big data adoption. There have also been discussions about changing the constitution to increase Japan's cyberdefense as well as traditional military defense capabilities.

These recent developments are likely to have far-reaching effects on the economic, political, and military institutions of the world's third-largest economy. To effectively protect Japan's digital assets and IT infrastructure, IT professionals and business executives need an informed understanding of key elements of these changes. An analysis of the country's cybersecurity dynamics highlights the major challenges Japan faces in strengthening cybersecurity and the differences between its approach and those of other major world economies.

GROWING CYBERSECURITY AWARENESS

Of Japan's 11 political parties, only 3 included statements about cybersecurity in their manifestoes for the Upper House Diet election in 2010 (http://tinyurl.com/k4rgawn). However, the 2011 cyberattacks against the Diet as well as defense contractor Mitsubishi Heavy Industries were eye-opening events to both policymakers and business executives. According to Mitsubishi, the perpetrators gained access to 83 computers and servers at 11 locations including its Tokyo headquarters, many factories, and an R&D center (http://tinyurl.com/n5sorx9). Other defense contractors such as IHI and Kawasaki Heavy Industries reported similar intrusions.

The cyberattacks also aroused concerns about Japan's cyberdefense capabilities from its trading partners and military and political allies. For instance, US authorities fear that private or state-sponsored hackers could obtain secret data about American warships, military aircraft, and missiles built under license by Japanese companies.

In response to these concerns, the Japanese government is creating an extensive network of regulatory bodies and enforcement agencies that significantly expand the country's cybersecurity infrastructure beyond the Cabinet Secretariat's National Information Security Center, which was established in 2005 following a series of cyberattacks on the websites of numerous government ministries and agencies in 2000 (http://tinyurl.com/n8fh7eg).

A key aspect of this effort is the ongoing attempt by the Liberal Democratic Party (LDP), which took power in 2012, to alter Article 9 of the Japanese Constitution to renounce the self-imposed ban on collective self-defense and thereby sanction counterattacks against foreign enemies. The LDP government argues that the proposed change would not only enhance its physical security against potential antagonists such as China and North Korea, but would also improve cyberspace security, which is critical to the country's economic prosperity.

In addition to cyberwarfare, espionage, and the theft of trade secrets, Japanese authorities are concerned about organized crime syndicates, which in recent years have shifted to cybercrime as the worldwide financial crisis and enhanced policing efforts have sharply curtailed revenues from traditional criminal activities (http://tinyurl.com/bwgw2ke).

JAPAN'S CYBERSECURITY EFFORTS

Japan's cybersecurity efforts fall into four broad categories: anti-cybercrime initiatives led by the National Police Agency (NPA); industry protection policies spearheaded by the Ministry of Economy, Trade, and Industry (METI) and the Ministry of Internal Affairs and Communications (MIAC); and national security measures coordinated by the Ministry of Defense (MoD). Academic institutions and the private sector are also working together to promote cybersecurity.

Anti-cybercrime initiatives

In 2004, the NPA installed a Cybercrime Division as well as a High-Tech Crime Technology Division in each prefectural Info-Communications Department. In March 2013, it announced the launch of a nationwide cybercrime task force consisting of 140 staff members. The NPA also plays a key role in public education about the importance of cybersecurity.

Industry protection policies

In November 2012, as part of its IT Integration Forum initiative established earlier that year, METI created the Personal Data Working Group. The group's report, released in May 2013, recommended using information-providing intermediary organizations to help "build a new relationship of trust between businesses and consumers for utilizing personal data." The working group also said that companies, instead of requiring consumers to disclose designated personal information to use any of their services, should provide different levels of services based on the type of data consumers want to disclose (http://tinyurl.com/mlp94t6).

Also in November 2012, MIAC convened the Research Society for Use and Circulation of Personal Data. The group's official report, released in June 2013, advocated transparency, user participation, and proper means of data collection and management of user information, among other things (http://tinyurl.com/k3dyhex).

National security measures

The Japanese government recognizes that ensuring cyberspace stability is critical to the mission readiness of the country's Self-Defense Forces (SDF). In April 2013, the MoD announced that by March 2014 it would set up a new Cyber Defense Unit (CDU) within the SDF with an operating budget of US$142 million (http://tinyurl.com/l5b5wbf). The CDU's key goals include protecting the SDF's information systems and contributing to the government's response to cyberthreats by advancing relevant knowledge and skills. A 100-person staff will be responsible for collecting data about malware and viruses and identifying ways to respond to cyberthreats.

Japan also actively cooperates with other nations to promote cyberdefense capabilities. For instance, it's working with the US to revise the two allies' Cold War era treaty guidelines to enhance information security (http://tinyurl.com/o7qw6j6) and plans to conduct joint cybersecurity drills with Russia (http://tinyurl.com/kwtpesw).

Academia and the private sector

A report on long-term cybersecurity strategy released in mid-2013 by a government panel of experts emphasized the need to upgrade specialized education at universities and other institutions to strengthen human and technological capabilities in cybersecurity and to boost the number of IT security engineers in the country (http://tinyurl.com/pcm2cye).

In addition, Japanese universities are collaborating with companies to increase cybersecurity awareness. In May 2013, for example, Keio University hosted the Microsoft-sponsored Asia Forum on Cyber Security and Privacy (http://tinyurl.com/mzsqhc9).

Japanese businesses are also partnering with other corporations with cybersecurity expertise to provide cybersecurity training and solutions. In September 2012, for example, Sojitz inked a deal with Boeing "to help defend Japan's information technology infrastructure from sophisticated, evolving, and persistent cyberattacks" (http://tinyurl.com/l7hflf4).

INSTITUTIONAL AND SOCIOLOGICAL CHALLENGES

Despite these efforts and greater awareness of the importance of cybersecurity, Japan faces many obstacles implementing robust measures.

One major challenge is the government's longstanding reluctance to invest in cybersecurity (http://tinyurl.com/l5b5wbf). For example, from 2006 to 2010, while many countries were steadily increasing R&D spending, Japanese cut such spending by nearly 50 percent. In comparison, South Korea's cybersecurity investment is significantly larger; in July 2013, it announced that it was doubling its cybersecurity budget to 10 trillion won ($US8.76 billion) and hoped to train 5,000 IT security experts by 2017 (http://tinyurl.com/jwfmvdw).

Japan also suffers from insufficient and underqualified human resources. According to the Information-technology Promotion Agency, Japan faces a shortage of at least 80,000 IT experts and, among the country's 265,000 experts, 160,000 need additional education and training (http://tinyurl.com/l2d4bkd). The problem is exemplified by MoD's difficulty finding capable analysts for its planned 100-member CDU (http://tinyurl.com/kzfqzs7). One Japanese security specialist argues that the CDU's staff is likely to be recruited internally from among SDF personnel who lack sufficient computing skills as well as a "cyberwarrior mentality" and maintains that the CDU needs at least 2,000-3,000 dedicated cybersecurity specialists (http://tinyurl.com/l5b5wbf).

Sociological factors are equally important. A senior fellow at Tokyo's Center for International Public Policy Studies notes that, in common with other professionals, Japanese cybersecurity specialists seek lifetime employment. In highly mobile job markets such as in the US, however, workers frequently move among the public sector, private sector, and academia, which facilitates the institutional transfer of IT skills. Moreover, unlike US government agencies like the FBI and NSA, Japan is wary about hiring hackers (http://tinyurl.com/lnyy4tl).

COMPARISON WITH OTHER COUNTRIES

As Figure 1 shows, there are key similarities with and differences between Japan's cybersecurity approach and those of the EU and US.

	European Union	United States
Similarities	Comprehensive regulatory framework that applies across all sectors	To some extent relies on private-sector self-regulation to ensure privacy and protect data
	Concerned about privacy and data protection; limits imposed on cloud computing and big data	Faces common cyberthreats from foreign countries
Differences	Collection, processing, and transfer of personal data by enterprises doesn't require user consent	Doesn't have a consumer-protection agency equivalent to the US Federal Trade Commission
	Businesses have no general obligation to delete personal data after use	Low job mobility of cybersecurity specialists across the public sector, private sector, and academia
	Companies providing online services don't have to report cyberattacks	

Figure 1. Key similarities with and differences between Japan's cybersecurity approach and those of the EU and US.

European Union

Like the EU, Japan has a detailed, comprehensive regulatory framework that applies across all sectors. In addition, it shares the EU's concerns about privacy and data protection and thus similarly limits cloud computing and big data services (http://tinyurl.com/kevjxa6). In this regard, recommendations by METI's Personal Data Working Group, MIAC's Research Society for Use and Circulation of Personal Data, and other interested bodies encourage the government to ease such restrictions so that society might benefit from these technological advances.

There are also key differences between Japan and the EU with respect to cybersecurity. While the EU mandates that companies obtain users' consent to the collection, processing, and transfer of personal data (http://tinyurl.com/la8nonn), Japan only requires enterprises to state the purpose of using such data—user consent isn't necessary. Likewise, Japanese businesses have no general obligation to delete personal data after use. Finally, unlike the EU, companies offering online services in Japan aren't required to report cyberattacks.

United States

Japan, like the US, relies to some extent on private-sector self-regulation to ensure privacy and protect data. The Personal Information Protection Law, enacted in 2005, obligates companies

handling personal data of 5,000 or more individuals to take "necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data" (http://tinyurl.com/lp4zrz3). Failure to comply with the law is punishable by a fine up to ¥300,000 (about US$3,000) or imprisonment for up to six months.

Japan also faces common cyberthreats with the US, which encourages the two countries to work more closely together. The 2011 cyberattacks against Japan, which coincided with the 80th anniversary of the Manchurian Incident, allegedly originated from China (http://tinyurl.com/438fogl), and there is strong evidence that hackers either working directly for the Chinese government or with their sponsorship are targeting government agencies and private companies in both Japan and the US to steal sensitive data (http://tinyurl.com/kxzk73w).

On the other hand, Japan doesn't have a consumer-protection agency equivalent to the US Federal Trade Commission. METI provides various data protection and privacy guidelines, but, while most businesses comply with these guidelines, they're not legally binding.

In recent years, Japan has initiated significant measures to boost cybersecurity. Compared to other advanced economies, however, its efforts still fall short of what's needed to effectively deal with an increasingly sophisticated array of cyberthreats. Nevertheless, government officials and the public have become more aware of the importance of cybersecurity, and Japan is now taking more aggressive steps to address this deficiency.