RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 018 – 29 January 2020

Cybersecurity Framework: Addressing Japan's Manpower Crunch

By Mihoko Matsubara

SYNOPSIS

The shortage of cybersecurity professionals is a worldwide challenge. How do Japanese companies address this problem? They have launched their first cross-sector industry forum that uses global frameworks as a common language to communicate.

COMMENTARY

THE CURRENT cyber threat landscape remains grim: the world struggles to keep up with growing cyberattacks. According to NTT Corporation, a major ICT service provider in Tokyo, 44 percent of companies have experienced a breach in 2019; the estimated costs of recovering from a breach continue to increase from 9.9 percent of their revenue in 2017 to 12.7 percent in 2019.

That is why cybersecurity professionals are in high demand to enhance cybersecurity. Yet, there is an acute shortage of cybersecurity talents. Cybersecurity Ventures predicts there will be 3.5 million unfilled cybersecurity jobs by 2021.

Pressure Will Grow

The pressure to improve cybersecurity is greater when a country is preparing for a major international event such as Olympic Games because their success requires both cyber and physical security. Tokyo was selected to host the 2020 Summer Olympic and Paralympic Games in 2013.

This has prompted Japan to strengthen its national cybersecurity capabilities and cultivate cybersecurity talents, because it is crucial to manage any potential

reputational and cyber risks and ensure to leave a positive legacy for future generations.

In the Internet of Things (IoT) era, cross-sectoral collaboration is becoming more important to obtain collective knowledge and tackle with cyberattacks. That is why Japanese industry decided to form the Cross-Sector Forum to establish a good ecosystem to educate, recruit, retain, and train cybersecurity professionals in collaboration with academia and government.

In April 2015, then Senior Executive Vice President Hiromichi Shinohara of NTT, started to talk to his senior counterparts at Japanese critical infrastructure companies to urge them to launch a forum.

The Cross-Sector Forum

Finally in June 2015, the forum was founded with 30 major companies from all the critical infrastructure sectors including chemical, financial, manufacturing, media, and transportation. As of today, the forum has 44 members in total.

It was groundbreaking for Japanese industry to create a cross-sector cooperative framework on their own voluntarily to influence policy and share best practices rather than waiting for instructions from the government.

Still, the forum members initially faced difficulties in having frank and open discussions between different critical infrastructure sectors due to their different business culture before they build trust over many face-to-face meetings and after-work drinks. The forum first had to define what cybersecurity professionals and their missions mean to end-user companies.

Since all the members have a global business presence and one-fourth of them are Tokyo 2020 sponsors, the members agreed to adopt a global common language rather than a domestic one, so that they can bring back their findings to their subsidiaries outside Japan.

Thus, the forum began looking for a global cybersecurity standard for the protection of critical infrastructure and found the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Because the Japanese Information-Technology Promotion Agency (IPA) published a Japanese translated version in May 2014, it became easier for the Japanese forum members to understand the framework to have a holistic picture to map what cybersecurity missions end users should pursue.

NICE Framework: For In-house Cyberscurity

The forum had to overcome another challenge due to their unique business culture. Under the lifetime employment system, major Japanese companies traditionally rotate their employees every two to three years. This helps employees understand the whole picture of the company business but makes it difficult to maintain cybersecurity expertise and keep up with ever-growing cybersecurity issues.

Only 28% of IT professionals work in-house in Japan, whereas 65% do so in the US and 54% in the UK. Japanese end-user companies tend to outsource most IT and cybersecurity work to system integrators and vendors.

The outsourcing culture made the forum pick another global standard, the National Initiative for Cybersecurity Education (NICE) Framework to define skills, which Japanese end user companies typically outsource, such as digital forensics to fulfill their missions. The NIST Cybersecurity Framework was used to map missions for in-house cybersecurity positions.

The forum has published a chart to map different types of cybersecurity jobs from Chief Information Security Officer and auditors to hands-on technical people such as Security Operation Center people and Help Desk, and shows how deep technical knowledge is needed to do their job.

Another chart defines what kind of skillsets are needed for so-called operational technology (OT) people, who specialise in industrial control systems for critical infrastructure, based on NIST 800-53 Rev. 5 (draft): Security and Privacy Controls for Information Systems and Organizations.

NISC: For Policymakers and Educators

The forum members also reached out to the Japanese government and universities to incorporate industry's efforts to cultivate cybersecurity professionals into policy-making and education. The National center of Incident readiness and Strategy for Cybersecurity (NISC), which is responsible to make national cybersecurity strategy and policy, as well as the Ministry of Economy, Trade and Industry invites the forum to their strategy committee meetings and ask the forum to share their findings.

Japanese national strategies refer to the Cross-Sector Forum, introducing their definition of cybersecurity professionals. Furthermore, some of the forum members fund universities to create a cybersecurity course and send their employees as lecturers to share their first-hand knowledge to detect, analyze, and response to cyberattacks.

Efforts the forum makes are not just limited to Japan. They participate in international conferences such as ones hosted by NIST to share how the Cross-Sector Forum uniquely utilizes the NIST and NICE Frameworks to define cybersecurity missions and professionals. Since some members have the market in Southeast Asia, they are actively involved in cybersecurity capacity-building.

For example, one of the forum members provided train of trainers for a national Computer Emergency Response Team (CERT) so that the CERT can conduct further training for local critical infrastructure companies. Another member hosted a number of cyber exercises and incident response training for ASEAN countries.

Their journey to define cybersecurity missions and talents has helped the Cross-Sector Forum better communicate with the international cybersecurity community because they are now equipped with a global common language. This also allows the

forum to share their learnings to adopt global standards and contribute to capacity-building domestically and internationally.

Because ASEAN is now expanding its investments in cybersecurity capacity-building, the forum's projects are topical and relevant to ASEAN countries. It is the time for Japanese industry to offer its insights to the region and contribute to better cyber resiliency in the world.

Mihoko Matsubara, Chief Cybersecurity Strategist at NTT Corporation, contributed this specially to RSIS Commentary. She previously worked at the Japanese Ministry of Defence, Hitachi Systems as a cybersecurity analyst, Intel Corporation as Cyber Security Policy Director, Palo Alto Networks as Chief Security Officer (CSO) in Japan and Vice President & Public Sector CSO for Asia-Pacific in Singapore. She is also an Adjunct Fellow at Pacific Forum, Honolulu, and an Associate Fellow at Henry Jackson Society, London.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg