PACNET

INDUSTRY COOPERATION UPLIFTS JAPAN'S CYBERSECURITY—AND MAYBE THE WORLD'S

BY MIHOKO MATSUBARA

Mihoko Matsubara (mihoko.matsubara.er@hco.ntt.co.jp) is Chief Cybersecurity Strategist, NTT Corporation, Tokyo, responsible for cybersecurity thought leadership. She worked at the Japanese Ministry of Defense before her MA at the Johns Hopkins School of Advanced International Studies on Fulbright. She is Adjunct Fellow at the Pacific Forum, Honolulu, and Associate Fellow at the Henry Jackson Society, London.

Cyberattacks have been growing increasingly frequent and sophisticated in recent years. Cybercriminals and cyber spies are taking advantage of the Covid-19 pandemic to launch more attacks, as the new normal has made organizations more reliant on information technology (IT), including cloud tools and web conferences. The attack surface has expanded drastically.

But along with the increased frequency of cyberattacks to disrupt business operations or steal intellectual property and national security secrets, the world also faces an acute shortage of cybersecurity professionals. The (ISC)^2 Cybersecurity Workforce Study 2019 revealed the world is short 4.07 million cybersecurity professionals, and 51% of surveyed cybersecurity professionals are concerned as to whether their employer is at "moderate or extreme risk due to cybersecurity staff shortage." Given this international situation, global supply chain risk management is a must to protect businesses, critical infrastructure, international trade, and national security. Employers need to have people who can incorporate cybersecurity into their business processes and help ensure the robustness of global supply chains.

The 2018 Japanese Cybersecurity Strategy addresses this urgent need to develop cybersecurity talent and create a wide variety of cybersecurity curricula for all ages, from elementary school students to young professionals to senior executives. Japanese industry has accelerated its cybersecurity efforts over the past several years. Still, it is expensive for companies to create cybersecurity training programs, along with curricula, as new cyberattack methods and cybersecurity technologies are always emerging.

Of course, multiple vendors around the world offer cybersecurity training programs, but as of yet there are no standardized international cybersecurity training syllabi. As such, there is a need to create internationally accepted or recognized syllabi to allow global companies to more easily choose cybersecurity training programs for specific skills and help to lower the price of training.

That is why FUJITSU, Hitachi, Ltd., and NEC Corporation, three major Japan-based global information and communication technology (ICT) service providers, declared in December 2017 that they will develop common cybersecurity syllabi together. "Cyber ranges" are popular virtual platforms offering an authentic and real-world IT environment for hands-on training of cybersecurity professionals. Many companies find cyber range training unaffordable because curricula are highly tailored and a few vendors are currently available, but these three Japanese companies believed standardized cybersecurity training could be made more accessible and reasonably priced for everyone. They embarked on a multi-phase process to achieve this goal.

The first step the three companies took was to map what types of cybersecurity professionals they needed, based on the US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (SP800-181). Because the three companies have a global business presence, they chose the NICE standard as an international common language to more efficiently manage cybersecurity professionals around the world. It took about three months to map which types of cybersecurity professionals need to obtain which types of abilities, knowledge, and skills.

Second, the companies developed cybersecurity curricula for what they identified as the four highest priority cybersecurity professional categories: penetration testers, forensic engineers, incident responders, and security operators. Concluding in October 2018, it took one year to create a prototype for the four categories. Closing the gaps was challenging because each of the three companies was accustomed to different terminologies and had different priorities for their cybersecurity professionals.

Third, the three companies took part in discussions with the Cyber Risk Intelligence Center (CRIC), a non-profit consortium based in Tokyo, to share cybersecurity best practices with the world. Hitachi and NEC, along with Nippon Telegraph and Telephone Corporation (NTT), founded the Cross-Sector Forum in June 2015 to create an ecosystem for educating, hiring, training, and retaining cybersecurity professionals. FUJITSU is one of the 43 Forum members. The Cross-Sector Forum joined the CRIC in April 2017. These three companies believe that the Center is an ideal platform to discuss the development of cybersecurity professionals and standardized cybersecurity training curricula in an open manner with other ICT companies and cybersecurity vendors.

Because these companies collaborated to compare notes about their own cybersecurity training, they've been able to gather best practices to nurture cybersecurity professionals more broadly. This journey has allowed the companies to develop standardized cybersecurity training syllabi, and once a volume discount becomes available, more companies will be able to train their employees.

By the end of 2019, NTT, as a member of the CRIC, has twice conducted cybersecurity training workshop trials based on prototype syllabi. These experiments proved the trial curricula would allow companies to conduct training at lower costs. Afterward, the trainees offered feedback on how to revise the syllabi to improve future training sessions.

The Covid-19 pandemic has introduced challenges to cybersecurity training based on the new syllabi. NTT had planned to start modified cybersecurity training workshops based on the feedback shortly after April 2020, the beginning of the Japanese fiscal year. Nevertheless, the Covid-19 outbreak and state of emergency between April and May 2020 prevented NTT from hosting in-person workshops.

Online training is not ideal because instructors need to pay close attention to trainees, observing their reactions and the commands they type on screen. It is also necessary for instructors to adjust the content and speed of training for each student. Despite these challenges the companies, including NTT, plan to make some of the training program available online in fall of 2020 to accommodate wide-spread remote working during the pandemic. To ensure quality results, online training instructors will need to maintain close communication with individual students, interacting to simulate in-person training as closely as possible.

In the meantime, the next step for the CRIC will be the development of cybersecurity syllabi for the 10 remaining professional categories such as security auditor and consultant. Subsequently, they can share the newly added standardized syllabi with its members.

A final step in realizing this vision will be the global expansion of the standardized cybersecurity training syllabi. Because CRIC members necessarily have business operations outside Japan, these companies must strengthen global cybersecurity resilience and conduct cybersecurity training for all employees. NTT has translated the cybersecurity syllabi from Japanese to English. Standardized cybersecurity training curricula becoming internationally available will facilitate the pipeline generation of next-generation cybersecurity engineers.

As Japan is an aging society with a decreasing birthrate, its companies have had to invest more in the global market. Accordingly, the volume of mergers and acquisitions (M&A) of non-Japanese businesses has skyrocketed since 2013. As a result, this rapid M&A growth has made cybersecurity governance more complicated. Cybersecurity expectations and use of cybersecurity-related products and services vary significantly among nations and companies. This makes it challenging to manage and operate

cybersecurity across the globe and maintain integrated visibility to tackle cyber risks. The need to standardize is growing nevertheless.

This is why it is crucial to start preparing to widen cybersecurity training syllabi beyond Japan, in both Japanese and English, by inviting non-Japanese companies to join. Fragmented cybersecurity efforts inhibit companies from more-proactively and expediently addressing borderless cyber threats. Additionally, the expansion of syllabi users would bring down the price of training in the long run around the world. Lastly, participation by non-Japanese companies will allow cybersecurity training developers to incorporate both Japanese and global perspectives to make the syllabi truly international and standardized.