NIST

Cybersecurity Framework Success Story

Japan's Cross-Sector Forum

The voluntary Framework for Improving Critical Infrastructure Cybersecurity was developed through a collaborative process by industry, academia, and government stakeholders. It enables organizations – regardless of size, sector, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience. NIST does not validate or endorse any individual organization or its approach to using the Cybersecurity Framework.

Annual Cross-Sector Forum Conference for Executives

"Since the NIST Cybersecurity Framework is globally applied, it has helped the Cross-Sector Forum have a shared language among different industry sectors and facilitated our comprehensive discussions between member companies in Japan and their subsidiaries outside Japan."

- Koji Ueno, Chairperson

Benefits from Using the Framework:

- Since many Forum member companies have business operations both in and outside Japan and they sponsor the 2020 Tokyo Summer Olympic and Paralympic Games, the Cybersecurity Framework helps members to communicate with global cybersecurity professionals in government and industry in a globally shared language.

Situation

- In June 2015, NTT, NEC, and Hitachi took the initiative to launch the Cross-Sector Forum with major critical infrastructure companies from the chemical, financial, manufacturing, media, and transportation sectors in Japan to establish a good ecosystem to educate, recruit, retain, and train cybersecurity professionals in collaboration with academia and government.
- The Forum meets monthly and has four Committees: the cultivation of cybersecurity talents, the definition of cybersecurity talents, information sharing, and industry-academia collaboration. Each committee and the Steering Committee also meet monthly.
- As of September 2018, the Forum has about 40 members.

Drivers

- There are three differences between Japanese and U.S. companies in terms of cybersecurity professionals. First, Japanese companies still keep life-time employment and rotate their employees every two to three years. Thus, industry finds it challenging to keep up with fast-developing cybersecurity changes. Second, while 62.7 percent of Japanese companies have CISOs in 2017, they are mostly dual-hatted and they lack a firm cybersecurity background. That makes it especially crucial to assign experienced cybersecurity professionals to the CISO team. Third, Japanese end-user companies tend to outsource most IT and cybersecurity work to system integrators. Only 24.8% of IT professionals work in-house in Japan, whereas 71.5% do so in the U.S.
- Since the majority of the Forum members are end-user companies, they needed to define cybersecurity talent first.

Process

- Because of the Japanese business culture, two-to-three year rotation makes it challenging for employees to accumulate cybersecurity expertise. The Forum's Committee to Cultivate Cybersecurity Talents decided that it is better to identify what cybersecurity missions Japanese end-user companies need and, then, what cybersecurity skills are required to achieve them.
- First, the Committee prepared a questionnaire asking member companies about how their cybersecurity teams, such as the Information Systems Department, are structured.
- Second, the Committee started to look for a global rather than a domestic cybersecurity standard for the protection of critical infrastructure, seeking a unified language between different industry sectors since many members run their businesses in multiple countries. In May 2014, the Japanese Information-Technology Promotion Agency (IPA) published a version of the NIST Cybersecurity Framework translated into Japanese.
- Third, several member companies already had some knowledge about the NIST Cybersecurity Framework. They played a key role in mapping between how cybersecurity-related teams are structured and what missions and skills are needed. They used the Cybersecurity Framework as a global standard describing cybersecurity missions and terminologies applicable to any industry. Since the NIST Framework provides a holistic picture helping companies to determine what they should do, the Committee was able to make the map more comprehensive. This process took a few weeks.

Process (cont.)

- Fourth, the core members shared a mapping draft with the other members seeking their input within a month. Consolidating the input and reviewing a new draft was accomplished in another month.
- Fifth, the Committee began discussing which positions people execute and when and which cybersecurity work can be outsourced or not.
- In September 2016, the Forum published a final report of what it considers to be the First Stage of the process with three appendixes: the definition of cybersecurity talents, a calendar for executing cybersecurity missions, and a guide for conducting cybersecurity work in-house or for outsourcing.

The Forum used both the NIST Cybersecurity Framework and the National Initiative for Cybersecurity Education (NICE) Framework to map cybersecurity missions and skills. Since Japanese end-user companies usually outsource their cybersecurity work to system integrators, the Forum found skills listed in the NICE Framework, which are more technical, tend to be outsourced in Japan.

Here is the link to the mapping between the NIST Cybersecurity and NICE Frameworks in Japanese: http://cyber-risk.or.jp/sansanren/3.bessi_2_1.0.pdf.

To learn more about Japan's Cross-Sector Forum see: http://cyber-risk.or.jp/

Cybersecurity Framework Implementation Overview

Since the Forum members have subsidiaries outside Japan, the comprehensive NIST Cybersecurity Framework helped the members implement global cybersecurity practices regardless of their industry sector.

Once NIST notified the Forum of the mapping between the Cybersecurity Framework and COBIT and ISO/IEC 27001, which Japanese companies had been using, the core member companies used it to explain the Framework's relevance to their cybersecurity missions.

Results and Impacts

It was the first time Japanese industry worked in a cross-sector initiative to strategically address cybersecurity needs and to seek an impactful solution – rather than waiting for instructions from the government. The NIST Cybersecurity Framework provided the Cross-Sector Forum with a shared definition and understanding of cybersecurity talents. After the Forum published reports with their findings, the government began inviting the Forum to cybersecurity advisory panel meetings to incorporate their insights into Japanese cybersecurity strategy. Some member companies also started to sponsor cybersecurity classes for universities.

What's Next

As of September 2018, the Forum is developing a guidebook about how to use its publication defining cybersecurity talents, calendars for executing cybersecurity missions, and a guide to insource or outsource cybersecurity operations. The Forum is also creating a database of cybersecurity training programs available in Japan. Once the portal becomes available to the public, anyone will be able to add cybersecurity training programs, explaining how that program can help execute the missions and cultivate the skills associated with various cybersecurity positions.

Contact Information & Resources

Email address: office@cyber-risk.or.jp

Website: http://cyber-risk.or.jp/

Cybersecurity Framework website: https://www.nist.gov/cyberframework

NIST contact: cyberframework@nist.gov