Because of the Japanese business culture, the Forum
Since many Forum member companies have business
First, the Committee
There are three differences between Japanese and U
Since the majority of the Forum members are end
As of September 2018, the Forum ha
In June 2015, NTT, NEC, and Hitachi took the initiative to
Second, the Committee
Third,
Drivers
Situation
• In June 2015, NTT, NEC, and Hitachi took the initiative to
The Forum meets monthly and has four Committees: the
cybersecurity talents, information sharing, and industry-
Each committee and the Steering Committee also meet monthly.
• As of September 2018, the Forum has about 40 members.

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.

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.
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](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/](http://cyber-risk.or.jp/)

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/](http://cyber-risk.or.jp/)
Cybersecurity Framework website: https://www.nist.gov/cyberframework
NIST contact: cyberframework@nist.gov