INCENTIVIZING PRIVATE ENTITIES

HOW GOVERNMENT PROCUREMENT CAN BOOST CYBER SECURITY

PER CONCORDIAM ILLUSTRATION

By **Atsuko Sekiguchi**, deputy counselor, International Strategy Group, National center of Incident readiness and Strategy for Cybersecurity (NISC), and cabinet secretariat, government of Japan

Workforce development in the cyber security sphere is an urgent issue in Japan and across the world. According to the "(ISC)² Cybersecurity Workforce Study, 2019," the global shortage amounts to over 4 million workers. In the Asia Pacific area, the shortage is 64% of need. In Japan, the Asian-Oceanian Computing Industry Organization reported in 2018 that the shortage of capable talent reached 132,000 in 2016 and was expected to increase to 193,000 in 2020.

Out of respect for the autonomy of private entities, workforce development policy in Japan is implemented through voluntary initiatives. For instance, the cyber workforce has been developed under the 2018 Cybersecurity Strategy by raising awareness, enriching opportunities for education and capability development during careers, and the promotion of a certification system.

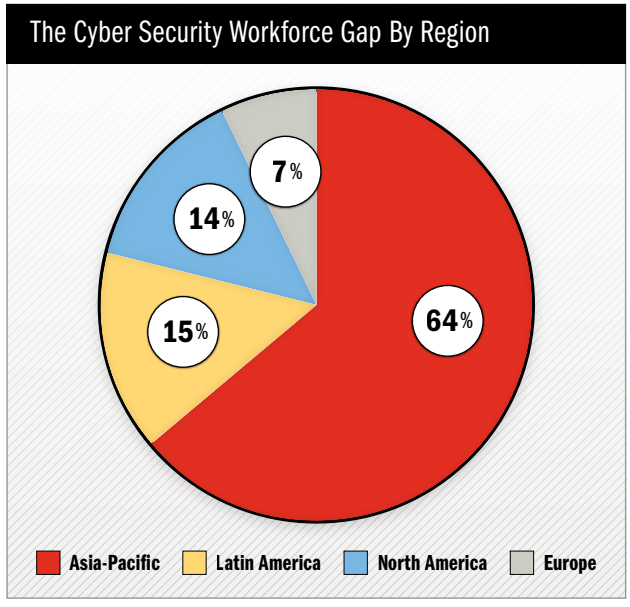
Yet, an insufficiency in the number of capable workers is widely recognized, showing the limitations of voluntary initiatives. One consideration for the enhancement of policy implementation could be an introduction of obligatory measures, such as the path taken in the United States, where the Executive Order on America's Cybersecurity Workforce issued in 2019 has been implemented. The order requires entities that participate in government procurement to deploy the National Initiative for Cybersecurity Education (NICE) framework that visualizes cyber security-related roles and encourages the career development of practitioners.

The first part of this essay explains current policy of workforce development for private entities in Japan and current data regarding the cyber security workforce. The second part shows the case for an obligatory effort to encourage workforce development, as deployed in the U.S. The last part is an examination on the applicability of this U.S. measure in Japan, resulting in a proposal suitable for the Japanese system.

THE SITUATION IN JAPAN

The historical basis of cyber security policy in Japan was the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society, passed in 2000, with Article 22 imposing a general obligation on the government to take measures to ensure security in telecommunications networks, which means that information security was merely a part of the legislation on the acceleration of digitization and that there was no reference to relevant stakeholders.

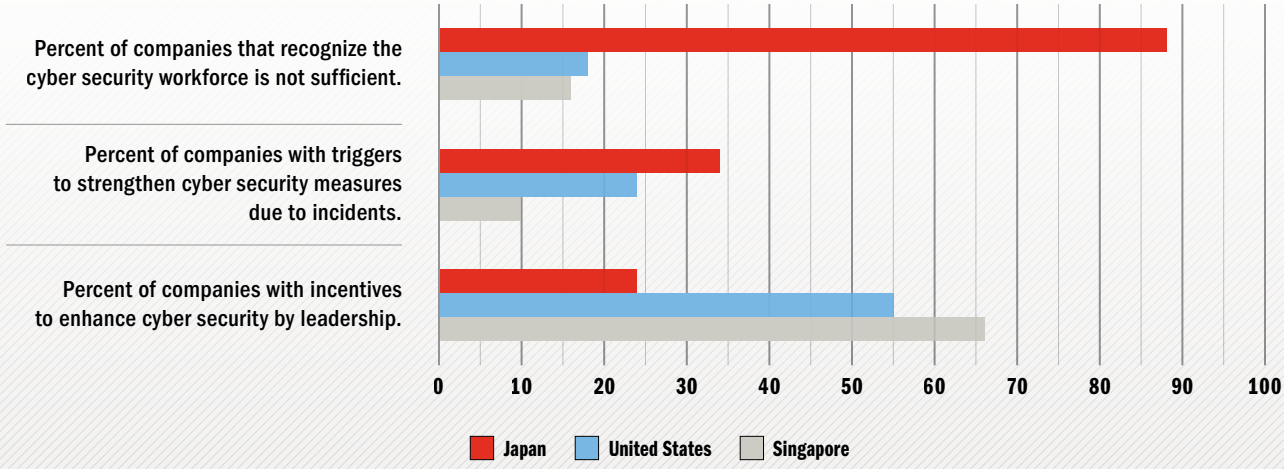
Japan's current cyber security policy stems from the Basic Act of Cybersecurity, passed in 2014. In that act, Article 4 requires the government to create and implement cyber security policy across the nation. Articles 6, 7 and 8 set the responsibility of critical infrastructure operators, private entities and cyber-related private organizations to cooperate with the government to achieve the goal of a national cyber security policy. Article 22 specifically requires the nation to take the necessary measures for workforce development in cyber security by ensuring appropriate rewards for professionals, utilizing certification systems, and providing education to the young via cooperation with educational institutions and private entities. This means that the law sets the responsibilities for each stakeholder relevant to workforce development, yet, respecting the autonomy of nonpublic organizations, it is not obligatory for private entities.



Source: Cybersecurity Workforce Study in 2019 issued by (ISC)²

The responsibility of the government is legally stipulated, yet specific measures are not stated within the legislation. As such, the Cybersecurity Strategy and related documents specify the direction of cyber security policy. The legislation requires that the Cybersecurity Strategic Headquarters (CH) be established as the highest authority of decision-making on cyber security policy, composed of

Comparison of Recognition Toward Cyber Security Among Japan, the U.S. and Singapore



Source: "NRI Secure Insight 2019"

relevant political figures, academics and private professionals, and it tasks the CH with setting cyber security strategy. Cybersecurity Strategy 2018, the most current, has three pillars: economic vitality, security of society and international stability. One section is devoted to workforce development as a cross-cutting measure supporting the pillars. The section points out that it is necessary to implement policy at all levels — in private entities, educational institutions and government. Related to the strategy, the CH instituted the Cybersecurity Workforce Development Initiative in 2018. The specific measures toward private organizations in this program are: changing the awareness of executives by disseminating the cyber security policy guidelines; providing opportunities for workers to reskill themselves and to develop their professional careers for management positions; and building technical capacity through a certification system. Therefore, the direction of the workforce development policy toward private entities is to create the appropriate environment to develop their awareness and skills.

In addition to statistics that show an estimated increase in Japan's workforce shortage, the "NRI Secure Insight 2019" study shows that 87.8% of companies in Japan recognize that the cyber security workforce is insufficient, while that same indicator is 18.1% in the U.S. and 16.3% in Singapore. The government of Japan has taken measures for workforce development by capacity building and educational opportunities, but there remains a wide recognition of deficiency.

Although the Japanese government is implementing policies to raise awareness within private entities, the NRI data shows that the motivation to raise the level of cyber security stems from actual damage from incidents, rather than leadership at the executive level. This raises questions about the current voluntary initiatives and whether they are sufficient to solve the inefficiency of human cyber resources in private entities.

THE U.S. EXAMPLE

The U.S. uses obligatory policies to enhance workforce development in cyber security. There are many projects within the private sector that follow three goals from the 2012 NICE Strategic Plan: Accelerate learning and skills development; nurture a diverse learning community; and guide career development and workforce planning. This was followed by the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure in 2017, which requires the secretary of Commerce and the secretary of Homeland Security to report on workforce development. One of the undertakings is the implementation of the NICE Cybersecurity Workforce Framework ("Special Publication 800-181") by the National Institute of Standards and Technology (NIST), which is part of the U.S. Department of Commerce, in order to visualize the capability of the cyber security workforce. The framework categorizes types of work into seven genres: security provision, operate and maintain, oversee and govern, protect and defend, analyze, collect and operate, and investigate. Within that, 33 specialty areas and 52 work roles are mapped. Additionally, at the regulatory level, the Executive Order on America's Cybersecurity Workforce, introduced in 2019, requires private entities that participate in government procurement to apply the framework within their organization in order to promote its utilization.

JAPAN AND THE OBLIGATORY APPROACH

Would the obligatory approach in the U.S. be appropriate in Japan? Regarding mapping capacity in the area of cyber security, the Cyber Risk Intelligence Center-Cross Sector Forum produced a Reference of Definitions of Human Resources in collaboration with the U.S. NICE. The forum is composed of several dozen indigenous companies and foreign subsidiaries from the chemical,

financial, manufacturing, media and transportation sectors. The reference outlines the tasks required to ensure cyber security, who is responsible for each task, and the level of knowledge necessary. The process of creating the reference enabled a common understanding of cyber security talents across sectors that have differing cultures and a varying use of terms on human resource development. Thus, Japan's framework on workforce in cyber security has been created by a private-driven organization and not by the government out of respect for the autonomy of private entities.

A website chronicles the successful collaboration between Japan's Cyber Risk Intelligence Center-Cross Sector Forum and the U.S. National Initiative for Cybersecurity Education, or NICE. NIST

The Common Standards for Information Security Measures for Government Agencies and Related Agencies (Common Standards) was established by the National center of Incident readiness and Strategy for Cybersecurity (NISC) based on Article 25 as a mandate from the CH to set a standard to evaluate measures taken by government agencies. Based on the documents, agencies set their own cyber security standard, and the NISC audits them to check whether the Common Standards are compiled regularly to ensure a certain level of security in government agencies. Section 4 imposes conditions that should be included in the government procurement process. Although the Common Standards contain technical conditions to prevent vulnerabilities within contacts between government agencies and private entities, the criteria do not include a condition on workforce development within private entities.

In summary, there are differences between the U.S. and Japan. In the U.S., a framework has been adapted within the process of government procurement to force private entities to accept the framework within their organizations. On the other hand, in Japan, the condition of government procurement does not involve the implementation of workforce development policy by private entities. Furthermore, although workforce mapping suitable for Japan's culture was produced, its application remains at the level of initiatives by private organizations. Thus, it is difficult and not appropriate to introduce the policy implemented in the U.S. to Japan, as many differences exist.

Additionally, requirements regarding workforce development pertaining to private entities within government procurement might lead to a discussion on whether this additional condition is allowed under World Trade Organization procurement provisions that cover nonessential conditions. The provisions limit the imposition of participatory conditions based on "legal and financial capacities and the commercial and technical abilities to undertake the relevant procurement." It remains an issue whether a workforce development requirement would comply, yet that question is not for this article to consider.

Although the deployment of the Reference of Definitions of Human Resources as an eligible requirement might not have been smooth in Japan, the government is able to carry out a comparative examination of applications from private entities in government procurement to ensure the quality of procured services. This involves several evaluative points, including the bidding price, the quality of a proposal and relevant experience to prioritize a bidder in terms of public interest. If workforce development measures, such as the deployment of the human resource framework, become part of the evaluation criteria in government procurement within the Common Standards, it will encourage private entities to make it a priority. It will also leave no doubt about conformity with the international trade regime as it encourages measures to be taken but does not exclude any entities to enter government procurement. In addition, it surely promotes the acceleration of workforce development measures within private entities beyond voluntary initiatives, and still respects the autonomy of the private sector, a principle of cyber security policy in Japan. Some might criticize the idea because the companies that can participate in government procurement do not amount to a large percentage of the nation's entities. However, it would be realistic for the government, as a first step, to incentivize private entities to deploy workforce development measures by making it one of the evaluation criteria within government procurement in the Common Standards. Furthermore, the proposal has the possibility to be expanded to other entities associated with the entity that participated in the government procurement.

CONCLUSION

One of the possible measures to incentivize private entities in Japan is to implement workforce development plans through a government procurement process, not simply by voluntary initiatives. The proposed solution might not be perfect for covering the whole of private entities immediately. Yet, this proposal will contribute to the discussion not only in Japan, but also in other nations on how a nation can take one step forward from voluntary initiatives in the area of cyber security workforce development to improve the situation for future generations. □

This article represents the author's views and not the position of the NISC, nor the government of Japan.