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

RSIS COMMENTARY

www.rsis.edu.sg
No. 121 – 18 July 2018

# Japan's New Cybersecurity Strategy: Plugging the IoT Gap

*By Mihoko Matsubara*

## Synopsis

*Japan should craft a new Cybersecurity Strategy to encourage risk-averse business leadership to tackle shadow IT and bring visibility and control on two key fronts: first, endpoint security to protect computers, servers, and wireless devices and second, cloud security to protect data, applications, and infrastructure of cloud computing.*

## Commentary

THE JAPANESE government released a draft of the next *Cybersecurity Strategy* in June 2018 to share its vision for strengthening Japan's cybersecurity capabilities for the coming few years. The new strategy draft is the first national security document in which endpoint security to defend computers, servers, and wireless devices is mentioned.

The inclusion of endpoint security showcases the hard lessons learned from the WannaCry incident in 2017. Japanese government and industry were both shocked that the WannaCry disrupted business operations in Japan, even for major Japanese manufacturers, not just foreign companies.

## Endpoint and Cloud Security

If the final Cybersecurity Strategy is to include a specific type of cybersecurity like endpoint security, it should also refer to cloud security to ensure comprehensive protection of IT resources, not just for the government but also for industry. The Strategy draft emphasises pursuing innovations through artificial intelligence and the Internet of Things (IoT) and taking security measures for private cloud for the government.

Big data is key to machine learning and IoT to create new business values and opportunities. IBM estimates that 2.5 quintillion bytes of data are created daily. To keep up with exploding data, it is impossible to remain dependent on computers on the premises (on-premises) is not as flexible and scalable as the cloud.

## IoT Adoption in Asia-Pacific vs. Japan

Yet Japanese companies have taken more time than other countries to introduce IoT and cloud services. The Vodafone IoT Barometer 2017/18 report shows that 36 percent of organisations in the Asia Pacific have implemented IoT, compared to 27 percent in the Americas and 26 percent in Europe. In contrast, the adoption ratio in Japan was only 12 percent, which the Asia-Pacific region achieved in 2013. As of 2016, 46.9 percent of Japanese companies use cloud computing for emails, data storage, and/or file sharing, whereas the adoption ratio was 70 percent in the United States.

There are a few reasons why IoT adoption in Japan is lagging. First, Japanese companies tend to begin conducting IoT proof of concept (POC) without setting a clear goal or deadline. They end up pursuing POC indefinitely rather than turning it into a new business operation. Second, compared to their counterparts in other countries, fewer Japanese business leaders understand the potential effects of the digital revolution on employment and work.

While only eight percent of non-Japanese business leaders do not know those impacts outside Japan, the ratio is 20 percent in Japan. Third, Japanese business leadership is becoming more risk averse, which makes it difficult to adopt new business models. Forty-three percent of Japanese business leaders were risk averse in 2014, and this ratio went up to 60 percent in 2016.

The Japanese government started to incentivise industry's investments in IoT this summer to reduce companies' corporate tax if they can prove their investments in IoT devices such as sensors and robots will increase productivity and cybersecurity. This movement can be a gamechanger to galvanize IoT and IoT security in Japan. It will also require Japanese industry to rethink how to use cloud to keep up with big data produced by IoT.

## Cloud in Japan

According to the Japanese Ministry of Internal Affairs and Communications' 2017 White Paper, 47.3 percent and 35.4 percent of Japanese companies responded that they do not use the cloud because they do not need to or they are concerned about cloud security, respectively. Still, employees acknowledge the convenience of cloud services. In fact, shadow IT poses a huge challenge to corporate governance and cybersecurity. Shadow IT refers to IT products and services that employees use within their organisation without explicit approval from their employer.

NRI Secure Technologies' "Cyber Security Trend Annual Review 2017" report shows that only 40.4 percent of Japanese companies believe they use software-as-a-service (SaaS). However, NRI Secure Technologies, Ltd. discovered that 61 percent of those companies use Office 365 and 58.6 percent use Dropbox. Corporate employees have begun to use such cloud services for accessibility and convenience, even though their IT team is not necessarily aware of such SaaS usage and cannot apply security to it.

Nevertheless, 42 percent of Japanese companies believe that SaaS usage is not an issue as long as employees use it carefully. This optimistic view of cloud security and governance has led to insufficient knowledge of cloud security solutions. For example, cloud access security broker (CASB) provides visibility, access control, and data protection.

Gartner expects that 85 percent of major companies will use CASB in the world by 2020, although less than five percent of companies use it as of 2016. Cloud Security Alliance's Japan Chapter revealed that 63 percent of Japanese companies do not know about CASB. Japan is in urgent need to raise awareness of cloud security and increase visibility of IT assets connected to the internet or in the cloud.

## Japan's New Cybersecurity Strategy

Japan is the third largest world economy and its economic prosperity and success largely rely on cybersecurity as IT resources are fundamental part of business activities including innovations. It is Japan's responsibility as an economic power and global leader to ensure comprehensive and robust cybersecurity. As WannaCry demonstrated, a cyberattack can have cascading impacts, and its damage may not be contained within one organization, one sector, or one country.

Since Japan started a new tax incentive for IoT investments, it is crucial for the new Cybersecurity Strategy to acknowledge the gap between Japan and other countries in cloud and IoT adoption and provide a vision of how Japan should accelerate its cybersecurity efforts.

The Strategy draft's referral to endpoint security sends a positive signal about Japan's commitment to cybersecurity and business continuity. Now it is time to craft a new Strategy to encourage risk-averse business leadership to tackle shadow IT and bring visibility and control to endpoint and cloud security.

*Mihoko Matsubara, an Adjunct Fellow at Pacific Forum, contributed this specially to RSIS Commentary. Starting her career with the Japanese Ministry of Defence, she later worked at 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.*