Japan's Cybersecurity Policy and Best Practices Recommended by TCS

Rapid development of digitalization has led to the widespread adoption of emerging technologies and has created new opportunities for many companies. Simultaneously, the integration of physical and cyber realms significantly increases cybersecurity risks. Recent attacks have compromised governments as well as businesses. They dramatically illustrate the proficiency and creativity of hackers. The impact of evolving technologies such as AI and IoT is immensely extensive. Malicious agents are targeting vulnerabilities as the full implications of evolving technologies remain unknown. There is no doubt that cybersecurity will increasingly become important as technologies pervade every aspect of society.

To ensure cybersecurity, it is imperative to create systems that control and mitigate cyberthreats, and establishing a resilient cybersecurity strategy is the first step.

This paper discusses Japan's new government-led cybersecurity strategy and the technology-driven business transformation known as "Business 4.0."

The government's strategy provides a framework for companies to build or review processes that mitigate cybersecurity risks. In order to make this the basis of cybersecurity, we will explain in detail the three approaches for various cybersecurity initiatives to be carried out autonomously, and operational guidelines for companies to operate these approaches in accordance with the government's strategy. We will also present the specific examples of countermeasures.

Being Amplified Threats with the Expansion of Cyberspace

Tokyo is gearing up to host one of the world's most prominent sporting events in 2020, less than a year away from now. The event, returning to the city for the first time since 1964, will be watched by a global audience, and emerging technologies such as AI, IoT, automation, and cloud will be widely adopted. These Business 4.0 technologies will play an important role in the event and their effect is expected to be profound. They will enhance the experience for participants and spectators but also significantly raise considerations around cybersecurity.

While taking advantage of improved productivity, efficiency, and agility from new Business 4.0 technologies, organizations must also be vigilant to cyberthreats. As previously mentioned, increased interconnectedness and the spread of the Internet have led to a convergence of physical and cyber realms. This integration significantly increases both the potential benefit to society and the opportunities for nefarious agents to abuse cyberspace. The risk of damage in real space is amplified by the expansion of cyberspace.

Growing Importance of Cybersecurity Planning

A cyber attack during an international winter-sports event in 2018 took down several hundred computers in the host country, knocking Internet and television systems offline for hours. As the country prepares for its moment in the spotlight in 2020, there is an urgent need for Japan to strengthen its cybersecurity.

The world of sports has adopted a wide variety of new technologies. Athletes wear IoT-enabled smart vests and rely on real-time analytics software to improve their performance. Scoring and timing systems are all digital. Audience mobility and identity screening are computerized. Critical public infrastructure such as electrical grids and telecommunication systems, along with aspects of supply chains and transport, all rely on technology.

The complex nature of this supply chain means that the number of potential targets is huge and the threat is widespread. The adoption of technology also brings vulnerability since it means that there is a possibility of becoming the target of cyberattacks. Prompt action is required to protect against that threat. The Japanese government is encouraging all businesses – whether directly part of the planning for the event in Tokyo or not – to take this opportunity to build or revisit their cybersecurity planning initiatives.

Japanese Government's Cybersecurity Strategy

Japan's government sees cyberspace as the next great frontier across which great value lies untapped, which is why its sustainable development and security are a national priority. The government is taking drastic measures to protect its netizens. One example is the unprecedented large-scale initiative called "NOTICE" (National Operation towards IoT Clean Environment) which launched a cyberattack on approximately 2 million devices in February 2019 to test the vulnerability of IoT devices on the Internet in Japan. Sensors, webcams, routers, etc., were targeted to prove that these devices are susceptible to attacks. As a result, approximately 90 million IP addresses of IoT devices were surveyed, and IDs and passwords were able to be entered for approximately 31,000 to 42,000 of those devices. In 147 of these cases, the cyberattack was even able to log in with an ID and password, drawing attention to the dire need for improved security. [i]

IoT devices tend to fall off an organization's operational management procedures and sometimes basic measures are not implemented for them - for example, passwords are used with default settings. In addition, due to their long life cycle, it may not be discovered for a long time even if a cyberattack has been in progress all along. In order to avoid this situation, it is important for not only IT administrators but also management staff who decide investments in system operation management to get involved in ensuring that the proper settings are made for IoT devices and that security measures are thoroughly in place.[ii]

Following the results of NOTICE, the government has formulated a comprehensive cybersecurity strategy for 2020.[iii] The aim is to improve the preparedness of critical infrastructure, and to encourage and incentivize all Japanese businesses to pursue best practices. Reforming cybersecurity within every private Japanese enterprise and supply chain is central to this plan.

Three Approaches to Best Practices

The mandate from the Japanese government is based on three broad approaches:

1) Mission Assurance for Service Providers

-Steady execution of operations and services-

Organization managers are expected to identify operations and services as their "mission." They must then work towards improving the reliability and cybersecurity of these services.

2) Risk Management

–Assessment of uncertainty and appropriate response-

This approach mandates organizations to minimize risks by identifying, analyzing, and evaluating risks according to their organization's "mission."

3) Participation, Coordination and Collaboration

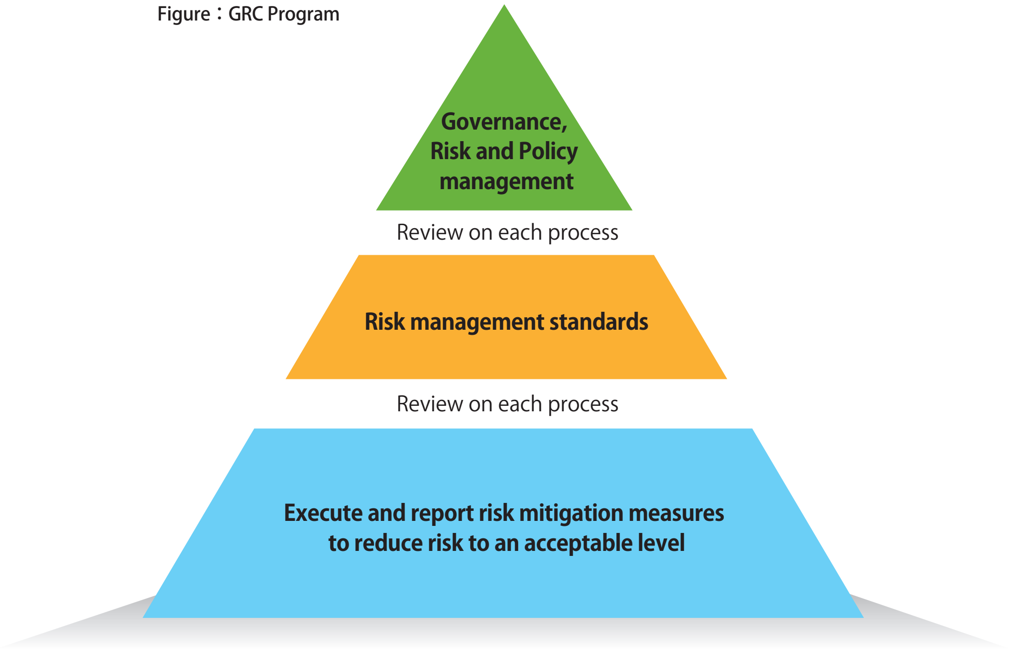
-Measures, coordination and collaboration by individuals and organizations in time of peace-

This approach expects organizations and individuals to implement measures in times of peace to prevent damage from cyberthreats and their escalation.

These three approaches provide a framework for scoping cybersecurity within individual enterprises. Aligning these approaches to current cybersecurity procedures will form the basis of next-gen best practices for Japanese businesses. Best practice implementation and compliance must be at the heart of corporate planning and investment.

Tata Consultancy Services (TCS) has created operational guidelines and specific examples of measures for companies to use these approaches. They explain matters such as the actions that managers should take, the need to establish a Chief Information Security Officer (CISO), and measures that CISOs should implement.

Figure：GRC Program


Governance, Risk and Policy management
Review on each process
Risk management standards
Review on each process
Execute and report risk mitigation measures to reduce risk to an acceptable level

Governance, Risk and Compliance Program

Realizing Best Practices as Recommended by TCS

In order for companies to realize the aforementioned approaches, investments need to be made in cyber resilience. Cyber resilience is the ability to quickly detect, respond to, and recover from damage that an organization fails to protect itself from during a cyber-attack. If organizations consider cybersecurity risks as part of their business risks, then cyber resilience can be established as part of their business continuity plans (BCPs) so that the countermeasure approach can be changed from a reactive approach to a predictive and preventive approach according to their BCPs.

A governance, risk and compliance program that maps the journey toward risk management must also be devised. Activities within the program must include the establishment of risk management policies, risk management standards, regular risk reviews, the implementation of risk mitigation to reduce risks to an acceptable level, reporting, and the establishment of overall cybersecurity governance. Considerations should also be made to deploy an IT GRC tool that automates the manual tasks of risk assessments, audit and control testing activities in order to further mature the risk and compliance program.

Supply chain risk is a part of risk management activities, and as partner ecosystems grow increasingly large to provide business services, so does the importance of supply chain risk. Hence, it becomes critical to assess and manage the risks from the third-party vendors. Attacks may occur due to the vulnerability of third-party systems. Organizations must assess and appropriately mitigate risks emanating from third parties in the supply chain. A "vendor risk management program" must be devised to formalize these activities. Product OEMs and service providers also become key entities in the overall supply chain. Organizations must guarantee that they are complying with security and privacy standards in their respective products and services.

A new cybersecurity strategy led by the Japanese government, formulated in preparation for the international sporting event to be held in Tokyo in 2020, is expected to mitigate various risks arising from cyberattacks not only during the event but also for many years to come. As one of the means to practice this, TCS uses the concept of "Business 4.0" to help organizations incorporate new and safe technologies into the organization's ecosystem, and also shore up corporate efforts to incorporate speedy management and technology in a flexible manner.

Takanori Sakayori
Cyber Security Head
Tata Consultancy Services Japan

Takanori Sakayori has been heading cyber security practice at Tata Consultancy Services Japan since April 2019. His experience includes networks (IT infrastructure engineer and project manager) and new business development, and more recently, he has led consulting projects for major Japanese companies, assisting them with cyber security assessment, development of roadmaps, and examination of cyber security measures.

Prashant D. Deo
Head of Asia Pacific Sales and Solution,
Cyber Security Practice
Tata Consultancy Services

Cyber Security Professional with 20+ year experience in Building and Managing large cyber security programs and cyber defense operations for global customers. He has been part of devising cyber security strategy for global organizations, setting up Computer Security Incident Response Team (C-SIRT) Programs, Advising customers to build cyber resilience programs and Performing Cyber Drills. He is currently managing Sales/Pre-Sales and solution function for APAC and Japanese customers.

[i] June 28, 2019 Ministry of Internal Affairs and Communications / National Institute of Information and Communications Technology / ICT-ISAC Press Release: Implementation of alerts to users of vulnerable IoT devices and IoT devices infected with malware

[ii] June 2019 Ministry of Internal Affairs and Communications: Implementation status of IoT device surveys and alerts

[iii] May 23, 2019 Cabinet Cybersecurity Strategy Headquarters: Cybersecurity 2019 (FY2018 report / FY2019 plan)