Japan's Quest to Attain SDGs Hinges on a Resilient Cybersecurity Ecosystem

INSIGHTS BY: GEORGIA EDELL
SECURITY ADVISORY CONSULTANT
FROST & SULLIVAN JAPAN

FROST & SULLIVAN

Powering clients to a future shaped by growth

The role of cybersecurity in achieving SDGs for Japan

It is imperative for Japan to develop a resilient cybersecurity ecosystem as the country emphasizes harnessing the full potential of technologies in its quest to attain The 2030 Agenda for Sustainable Development.

Japan's aggressive promotion of mission-oriented science, technology, and innovation (STI) policies presents a vivid roadmap for sustainable development goals (SDGs). With Japan's unique challenges—aging population and declining rural communities, the STI policy leverages technologies to catalyze innovation to drive SDGs, especially numbers nine (build resilient infrastructure), 11 (sustainable cities and communities), and 16 (peaceful and inclusive societies).

Additionally, the East Asian nation's vision for the future—Society 5.0—expedites the use of digital technologies such as the internet of things (IoT) and artificial intelligence (AI) to create human-centered society. The vision (Society 5.0) aligned with the UN's SDGs strikes a balance between economic development and resilience and well-being by integrating cyberspace and physical space to promote social transformation.

The massive use of immersive technologies, digital devices, and multiple applications to attain SDGs and Society 5.0 will increase cyber adversaries' activities in Japan's cyberspace. Such applications require an open network and easy accessibility to databases and applications, which expands attack surface by increasing exposure to cybercriminals. This compels the Government of Japan (GoJ) and concerned stakeholders to secure their data and systems.

Besides, Japan is prone to natural disasters, such as earthquakes and floods. Hence, it is essential for the country to build a robust digital infrastructure and adopt a resilient cybersecurity practices. It will help the nation to overcome such catastrophes and ensure the success of the SDGs, particularly numbers nine, 11, and 16.

SDG-9 (BUILD RESILIENT INFRASTRUCTURE): CLOUD SECURITY IS CRITICAL TO RESILIENT ICT

Natural disasters have plagued Japan for centuries. Due to climate change, the number and severity of catastrophes will likely increase in the coming years. As a result, the country must constantly seek ways to improve the resiliency of its infrastructure.

There is an effort to encourage resilient ICT to improve the physical resiliency of infrastructure. Natural calamities such as earthquakes and floods can destroy the country's physical infrastructure, including ICT-related infrastructure. The Resilient ICT Research Center, a part of the National Institute of Information Communication Technology (NICT), is researching this area. The center explores autopoietic (self-creating) edge clouds to solve unstable network connections during disasters. The technology essentially uses AI to create a cloud computing system that self-manages and adjusts resources autonomously to improve resiliency in case of an unstable connection.

Cloud security becomes critical as technology evolves to encourage resiliency, and its (cloud) adoption becomes even more ubiquitous. There is frequently misunderstanding about who is responsible for ensuring cloud security, and this lack of clarity leaves many enterprises vulnerable. Cloud service providers are responsible for protecting the cloud infrastructure, while customers are responsible for security in the cloud, including workloads, identity, data, and more. Awareness of a shared responsibility framework is vital to securing the cloud and achieving true sustainability.

SDG-11 (Sustainable cities and communities): Ensure cybersecurity in the physical use of ICT

Remote sensing and IoT devices are becoming more widespread to gather data and deliver insights. In the context of sustainable cities, these devices help provide data on:

- Weather—to help predict typhoons and mitigate heavy rainfall damage.
- Pollen dispersal and air pollution inform on changing air quality.
- The urban environment to give insight into people and traffic flows and congestion to provide data for urban planning and public safety.

These measurements and their indications can help develop sustainable and human-friendly cities. However, the function of IoT devices and sensors is to send data back to be processed and understood, making these devices key targets for hackers to gather digital data. Implementing IoT devices should be mandatory to protect these devices.

National Institute of Standards and Technology (NIST) outlines three risk mitigation goals to keep in mind when striving for cybersecurity:

1. **Protect device security**
2. **Protect data security**
3. **Protect individuals privacy**

The consideration of cybersecurity with the deployment of IoT devices can reap maximum benefits and mitigate data leaks.

SDG-16 (PEACEFUL AND INCLUSIVE SOCIETIES): CYBERSECURITY ITSELF CONTRIBUTES TO A MORE PEACEFUL, SUSTAINABLE WORLD

The internet has facilitated a truly connected world. According to the International Telecommunication Union (ITU) World Telecom Database, more than 90% of Japan’s population uses the internet, one of the highest rates in the world. However, increasing connectivity also expands the attack surface for cybercriminals.

A major difficulty with cybercrime is that no one is often held accountable. Cybercrime’s anonymity makes it more appealing, promoting further misuse. Further, inequality in cyber education and awareness means that certain groups are more likely to fall victim to cyberattacks, further widening the existing digital divide. Cyber security is critical to protect connected systems and encourage free exchange and connection without excessive risk of attack.

Investing in cybersecurity development and education is essential to upholding a democratic society and strengthening institutions and global standards. According to the Ministry of Internal Affairs and Communication’s survey in 2021, nearly 90% of respondents felt insecure when using the internet due to the threat of a leak of personal information. Japan should expand education efforts, especially around common attack vectors like email phishing. In this instance, digital education will enhance citizens’ knowledge and make them competent while surfing the internet. As a result, it will promote connectivity and inclusion and lead the country toward sustainability.

Conclusion

Japan's quest to meet Society 5.0 and SDGs has significantly increased the use of IoT and AI. The increasing online presence of concerned stakeholders and surging connectivity due to IoT devices expand the attack surfaces, thereby increasing exposure to cybercriminals. Additionally, the steeply rising trend of unprecedented ransomware attacks in the country in the past few years alarms the government to secure its cyberspace.

Besides cyber adversaries' attempt to disrupt Japan's cybersecurity space, the geological position of the country also encourages it to secure its digital infrastructure. As the country is prone to natural calamities such as frequent tremors and floods, Japan must develop a resilient and robust digital infrastructure. This will help the nation to overcome such catastrophes and ensure the success of Society 5.0 and SDGs.

Contact us:

Frost & Sullivan Japan
Akasaka Park Building,
5-2-20 Akasaka, Minato-Ku
Tokyo 107-6123 Japan
Tel:+81 50-6875-0901

Email: marketing.jp@frost.com

FROST & SULLIVAN

Growth is a journey. We are your guide.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion