

November 10, 2020

Toshiba to Present Cybersecurity Case Study for Critical Energy and Industrial Infrastructure in SANS ICS Asia Pacific Summit 2020

Singapore – Toshiba will be participating in [SANS ICS APAC Summit 2020](#) to address the topic of **‘Protect Power Plant and Industrial Infrastructure from Cyber Attack! ICS Security case study in Japan’** on 13 November 2020. Takashi Amano, General Manager, Cyber Security Centre at Toshiba Corporation, and Technology Executive, CISO, Toshiba Digital Solutions Corporation, will introduce the challenges and solutions in enhancing cyber resilience for power plants and industrial infrastructure, including a case study from Japan.

Cyberattacks are on the rise globally, with cyber threats targeting critical infrastructure such as power plants, wastewater facilities and industrial systems. The trend of digital transformation brought majority of industrial control systems and products that used to operate in closed environments to the internet directly or indirectly. However, connecting to the internet may expose the infrastructure to a greater risk of cyber threats, resulting in equipment damage, disruption of work processes, financial and intellectual property loss.

Toshiba is harnessing on its traditional and digital strengths to deliver cybersecurity solutions. One of the key solutions Toshiba offers to mitigate cyber attacks is to strengthen cyber resilience by tapping on the company’s manufacturing experience of over 140 years and applying its intelligence centric approach. The solution is currently applied in a power plant in Japan where visualization of assets and continuous monitoring are key. With a reduction in potential cyber threats, the power plant is able to allocate resources more efficiently, minimize disruptions to essential services, benefitting suppliers and ultimately end users downstream.

A sustainable, long-term security encompasses prediction and detection of security intrusion, corresponding response and recovery, evaluation and verification of up-to-the-minute security threats as well as channeling feedback to design and development processes. Added to this, is harnessing the benefits of artificial intelligence data collected to reduce the time required for and improve the accuracy of threat detection and response.

Toshiba aims to tap on cyber-physical systems (CPS) technology, where huge amounts of data collected from physical space in cyberspace in order to generate valuable intelligence and feeds it back to physical space. By enhancing the security of the cyberspace, it helps provide increased protection for the physical space. Combining a deep understanding of the physical space from decades of experience in manufacturing, with advanced cyber solutions, enables Toshiba to design a complete and well-rounded cybersecurity strategy as opposed to point solutions.

TOSHIBA

“Investment in cybersecurity is extremely vital to counteract the high cost, risk and downtime that comes with the disruption of an increasingly digitalized energy and industrial infrastructure sector,” said Takashi Amano, General Manager, Cyber Security Centre, Toshiba Corporation. “As a leader in cybersecurity solutions, Toshiba will showcase how cybersecurity technologies can help improve the cyber risk profile of critical infrastructure against cyberattacks.”

Toshiba will continue to contribute to the development of a safer digital economy in line with the United Nations Sustainable Development Goals (SDGs). By contributing from the angles of innovation, sustainability and partnership, Toshiba aims to provide cybersecurity solutions to minimize security risks from product design to manufacturing and operation, in the physical and cyber spaces.