FACTSHEET

SINGAPORE OPERATIONAL TECHNOLOGY (OT)
CYBERSECURITY MASTERPLAN

Operational Technology (OT) systems[1] were typically designed for monitoring and controlling physical processes, and are commonly found in sectors such as manufacturing, transportation, energy and water. These OT systems were historically isolated (i.e. not connected to the Internet) and were often not designed with robust cybersecurity considerations.

2 However in recent times, rapid digitalisation has led to the convergence of Information Technology (IT) and OT systems and created a vast network of systems interconnectivity. These previously isolated OT systems became susceptible to the same threat of cyber-attacks as IT systems. Given the cyber-physical nexus of OT systems, a cyber-attack against an OT system could have severe physical consequences, including mass disruptions, physical harm or even loss of lives.

3 Singapore is not immune to these global cyber threats. As Singapore moves towards being a Smart Nation, the underlying OT infrastructure systems, including those in the energy, water and transport sectors, are vital to support our Digital Economy and deliver essential services to Singapore and Singaporeans. We have to be vigilant to safeguard these systems and ensure a robust and resilient Smart Nation.

The Need for the OT Cybersecurity Masterplan in this Digital Age

4 The Cyber Security Agency of Singapore (CSA) has developed the OT Cybersecurity Masterplan as part of our continuous efforts to enhance the security and resilience of Singapore’s critical sectors delivering essential services; improve cross-sector response to mitigate cyber threats in the OT environment; and strengthen partnerships with industry and stakeholders. The OT Cybersecurity Masterplan which was launched by Senior Minister and Coordinating Minister for National Security, Mr Teo Chee Hean at the Singapore International Cyber Week on 1 October 2019, outlines key initiatives spanning the areas of “People”, “Process” and “Technology” to uplift the cybersecurity postures of our CII owners and organisations that operate OT systems. Key thrusts include:

a. Providing OT cybersecurity training to develop human capabilities
b. Facilitating the sharing of information through an OT Cybersecurity Information Sharing and Analysis Centre (OT-ISAC)
c. Strengthening OT owners’ policies and processes through the issuance of an OT Cybersecurity Code of Practice (CCoP)
d. Adopting technologies for system resilience through Public-Private Partnerships

[1] Operational Technology (OT) refers to technologies involving interconnected devices and computers for the monitoring and control of physical processes.

5 In addition, the Masterplan encourages OT equipment manufacturers and service providers to adopt cybersecurity-by-design in the developmental phase, so that products and systems are in-built with strong cybersecurity measures.

6 The OT Cybersecurity Masterplan will serve as a strategic blueprint to guide Singapore's efforts to foster a resilient and secure cyber environment for our OT CII; while taking a balanced approach between security requirements, rapid digitalisation and ease of conducting business-as-usual activities. The Masterplan will be available on CSA's website.

-END-