SCIC
SINGAPORE CHEMICAL INDUSTRY COUNCIL

Issue 56 Apr 2023

Pre-Digest

Cybersecurity in the Process Industry

Responsible Care®
OUR COMMITMENT TO SUSTAINABILITY

Feb 2021 - *Attempted poisoning of Florida's water supply via cyber intrusion*
May 2021 - *Colonial Pipeline hit by Darkside ransomware*
Jun 2022 – *Iranian steel mills operations taken over by hacker group*

In an increasingly connected world (physically and virtually), cybersecurity attackers are employing more sophisticated methods to achieve their objectives to infiltrate deeper into organisations and individuals. The cyber-attacks now cross over to the physical reality, which could result in operational disruption, financial & reputation losses and even process safety incidents!

1. Overview of Industrial Cybersecurity

Industrial cybersecurity, also known as OT (Operational Technology) cybersecurity, refers to the protection of operational technology systems, SCADA systems, and other systems used in industries. Operational Technology Systems are used to **Control**, **Monitor** and **Safeguard** the industrial process. These systems can include programmable logic controllers (PLCs), human-machine interfaces (HMIs), sensors, and other devices. These devices are vulnerable to cyber-attacks.

2. Cybersecurity Threats and Tactics used

The current threat landscape for industrial systems is constantly evolving, as cyber criminals are constantly finding new ways to exploit vulnerabilities in OT systems. Some of the different types of cyber threats that industrial systems may face include:

a) **Malware**: Type of software that is designed to harm or exploit computer systems. Example: Ransomware, trojans, and viruses.
b) **Phishing Attacks**: Phishing attacks are designed to trick users into divulging sensitive information, such as usernames and passwords.
c) **Social Engineering**: Social engineering attacks are designed to exploit human weaknesses to gain access to computer systems. Such as granting access to unauthorized users.
d) **Insider Threats**: Insider threats refer to attacks that are carried out by employees or contractors who have **authorized** access to industrial systems. These may involve stealing data or compromising systems.
e) **(DDoS) Attacks**: DDoS attacks are designed to overwhelm computer systems with traffic, causing them to slow down or become unavailable. It may cause operations disruption or equipment damage.

3. How to secure your organisation's OT environment?

DOs	DON'Ts
• Always perform virus scan of portable devices (e.g. USB sticks) before and after use in OT environment	• Charge portable devices (mobile phones) in OT systems
• Only use privileged accounts when necessary	• Share password or accounts with others
• Report any cyberattack threats, near-misses or incidents to company OT representative	• Ignore any errors, gaps and incidents in the OT systems
• Follow Management of Change process when changing OT systems / software	• Install non-approved software in OT systems
• Keep operating system patches and anti-virus up-to-date for devices connected to OT systems	• Use outdated patches and anti-virus versions

Useful links:
Cybersecurity Act 2018
Cyber Security Agency of Singapore

Process Safety is Everybody's Responsibility!

An initiative of the Process & Engineering Committee

SINGAPORE CHEMICAL INDUSTRY COUNCIL LIMITED (SCIC)
8 Jurong Town Hall Road, #25-04, The JTC Summit, Singapore 609434
Tel : 6267 8891 Fax : 6267 8893