SINGAPORE'S OPERATIONAL TECHNOLOGY CYBERSECURITY MASTERPLAN 2019

ACKNOWLEDGEMENTS

We would like to thank the OT community for their valuable input and support over the course of developing this Masterplan. In particular, we would like to specially mention the following individuals for their quotes provided in this publication, in alphabetical order of surname:

- **Mr. David Foo**,
  Senior Director, Operations Technology,
  Maritime and Port Authority of Singapore
- **Mr. Robert M. Lee**,
  Chief Executive Officer and Founder,
  Dragos, Inc.
- **Ms. Michelle Knight**,
  GM, Industrial Control Systems,
  Shell
- **Ms. Nathalie Marcotte**,
  SVP, Cybersecurity and Industry Services,
  Schneider Electric
- **Mr. Ng Joo Hee**,
  Chief Executive,
  Public Utilities Board
- **Mr. Ngiam Shih Chun**,
  Chief Executive,
  Energy Market Authority
- **Mr. Hiroshi Tanoguchi**,
  Head of Lifecycle Service Business Division,
  IA Systems & Service Business HQ,
  Yokogawa Electric Corporation
- **Mr. Donnie W. Wilburn**,
  IT Risk Management Manager,
  ExxonMobil Global Services Company
- **Mr. Shinichi Yokohama**,
  Chief Information Security Officer,
  NTT Corporation

TABLE OF CONTENTS

FOREWORD

Operational Technology (OT) systems, especially Industrial Control Systems (ICS), are an increasingly attractive target for highly-sophisticated cyber actors around the world. From the 2010 Stuxnet incident, the Ukraine power grid attack in 2015 to the recent ransomware that affected Norwegian firm Norsk Hydro, successful cyber-attacks on ICS have resulted in disruption of key infrastructure and essential services, as well as hefty financial losses. As we push towards our Smart Nation vision, Singapore, as a hyper-connected commercial hub, will need robust defences to fend off these advanced attackers.

The global trend of malicious attacks on OT systems shows no signs of abating. The threat is grave as OT forms the technological bedrock of our everyday lives and the economy, especially with the growing connectivity between Information Technology (IT) and OT systems. We rely on secure OT systems to regulate our traffic lights and rail networks, power our electricity grid and synchronise sensors monitoring our water supply, among other essential services.

It is therefore vital for Critical Information Infrastructure owners and regulators of these sectors in Singapore to constantly review and improve the cybersecurity posture of their ICS to ensure that their systems are secure and resilient. At our recent nationwide cyber exercise codenamed Ex CyberStar, CSA, together with all 11 CII sectors, was tested on complex cyber-attack scenarios including, for the first time, a widespread compromise of ICS. The exercise revealed certain areas for improvement in operations and processes.

CSA has launched the OT Cybersecurity Masterplan to create deeper awareness and understanding of the cybersecurity landscape; including the challenges faced by OT stakeholders from the public and private sectors. The Masterplan aims to consolidate and guide the development of OT cybersecurity initiatives to address key challenges, as well as mitigate the emerging threat vectors.

Cybersecurity is a collective responsibility – the government has taken the lead but we will also need everyone to play their part. We hope the OT Cybersecurity Masterplan will catalyse the collective development of localised capabilities and competencies in OT cybersecurity. To do so, CSA will work closely with our partners in the cybersecurity ecosystem and the industry sectors that own OT systems, toward a resilient OT cyber environment so that our people can enjoy the benefits and conveniences which technology brings.

David Koh
Commissioner of Cybersecurity and
Chief Executive
Cyber Security Agency of Singapore

EXECUTIVE SUMMARY

Operational Technology (OT) is integral to our everyday lives. The traffic lights controlling the flow of traffic, the signalling systems that regulates train deployment, and the electricity grid that powers up our appliances, are all managed by OT systems. However, such systems are often not designed with adequate cybersecurity in mind, and with the changes in the OT cyber threat landscape, new measures must be taken to secure our OT systems against cyber-attacks.

This OT Cybersecurity Masterplan, developed by the Cyber Security Agency of Singapore, aims to enhance the security and resilience of Singapore's essential service sectors, improve cross-sector response to mitigate cyber threats in the OT environment, and strengthen partnerships with industry and stakeholders. The Masterplan applies to both Critical Information Infrastructure (CII) owners that operate OT systems, as well as other enterprises that face the same OT threats and similar vulnerabilities. These include manufacturing plants in the oil and gas sector, semiconductor factories, and pharmaceutical companies, among others. In addition, the Masterplan will be useful for members of the OT cybersecurity industry, including equipment manufacturers, system integrators and penetration testers. It will help them better understand OT cybersecurity challenges, so that they can develop products and technologies that can be used by operators to strengthen the security of their OT systems.

To attain higher cybersecurity standards in the OT environment, the Masterplan focuses on enhancing the three main factors of People, Process, and Technology, through the following four key thrusts:

- **Enhance OT cybersecurity training** to raise CII sectors' preparedness through intermediate to advanced training courses offered by the CSA Academy and its training partners.

- **Set up an OT Cybersecurity Information Sharing and Analysis Centre** to facilitate threat information sharing among OT stakeholders in both the public and private sectors, allowing them to tap on the experiences and expertise from thousands of global organisations and share actionable cyber intelligence.

- **Strengthen OT cybersecurity policies and processes**, including prescribing measures in the OT Cybersecurity Code of Practice that provide cybersecurity controls and outcomes specific to OT systems.

- **Adopt innovative technologies for system resilience**, via the National Cybersecurity Research and Development Programme, industry calls for innovation and putting in place sectoral Security Operations Centres.

CSA will continue to work with our OT cybersecurity stakeholders, guided by the OT Cybersecurity Masterplan, to achieve a more resilient and secure OT environment to better serve Singapore.

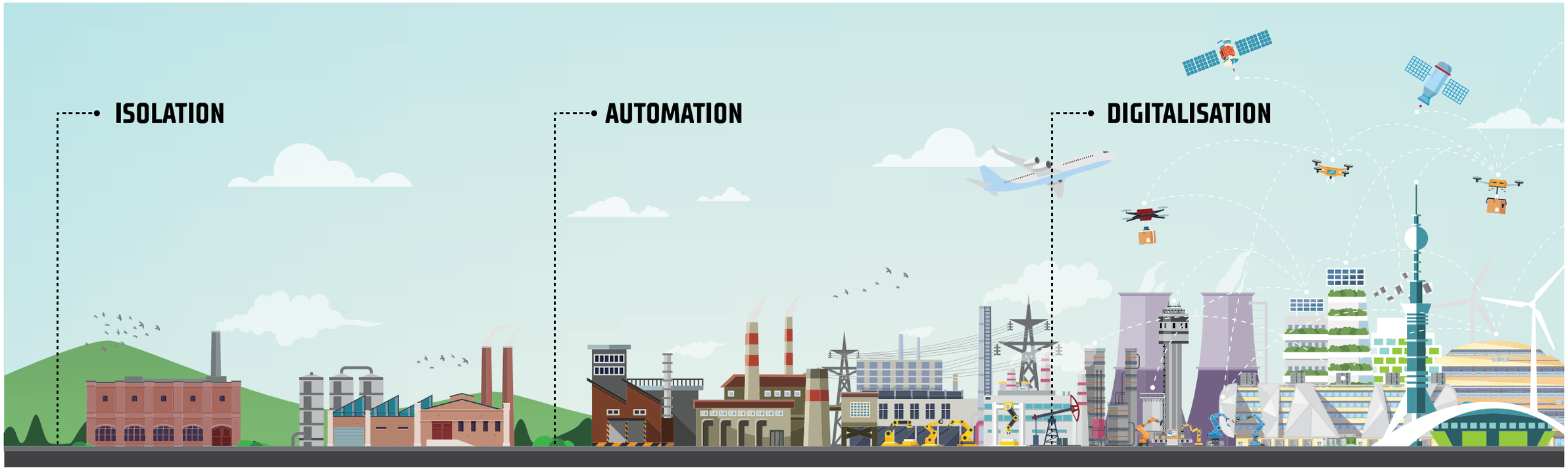
INTRODUCTION

What is Operational Technology?

Operational Technology (OT) refers to technologies involving interconnected devices and computers for the monitoring and control of physical processes. Today, OT is deployed in industrial sectors such as manufacturing, transportation, energy and water, among others.

OT is integral to our everyday lives. For example, the traffic lights controlling the flow of traffic, the signalling systems that regulates train deployment, the sensors detecting the chemical content in our drinking water, and the electricity grid that powers up our appliances, are all managed by OT systems. These systems effectively and seamlessly drive our modern way of life today.

EVOLUTION OF OPERATIONAL TECHNOLOGY IN THE AGE OF DIGITALISATION



Operational Technology has had a long evolutionary history. The control of industrial processes used to be managed by a complicated series of hard-wired relays, timers and sequencers, coupled with manual processes. OT systems arose out of a need to automate and digitalise these manual processes in order to enhance productivity and meet rising market demands for goods and services.

OT systems were designed to have a long life span, with a focus on reliability and safety, rather than security. These systems ran on proprietary control protocols using specialised hardware and software, and were often isolated from business networks and the Internet. This allowed OT systems to be "secure by obscurity", as they were typically not connected to and air-gapped from other systems. The possibility of a cyber-incident on OT systems was deemed to be remote due to the belief that their systems were completely isolated and air-gapped. In addition, OT systems were traditionally looked after by the engineering departments of companies, with little or no security considerations in mind.

Rapid digitalisation has caused industrial processes to shift from systems based on proprietary computing and communications, to those based on open standard Information Technology (IT) computing platforms. This has led to the convergence of IT and OT, and created an industrial revolution of systems interconnectivity.

Today, the extensive linkages among enterprise IT and OT networks, businesses, operators, vendors, and other third party systems have greatly increased the operational footprint of networks. OT systems are no longer air-gapped like before, and the cyber risk profiles of these systems have increased significantly. We need to ensure that cybersecurity measures to safeguard our OT systems evolve with the rise in cyber risks. The next section details the OT cyber threat landscape and how it affects Singapore.

Robert M. Lee
CEO and Founder,
Dragos, Inc.,
American ICS cybersecurity company

"As a community we have moved beyond the land of theoretical cyber-attacks on industrial operations to a world where these attacks are a reality for denying power, disrupting operations, and even specifically targeting human life as was the case in the TRISIS cyber-attack in 2017. The threat is worse than we realise but not as bad as we want to imagine. It is a worthy cause to invest in and prioritise OT cybersecurity and it is a winnable battle."

OT CYBER THREAT LANDSCAPE

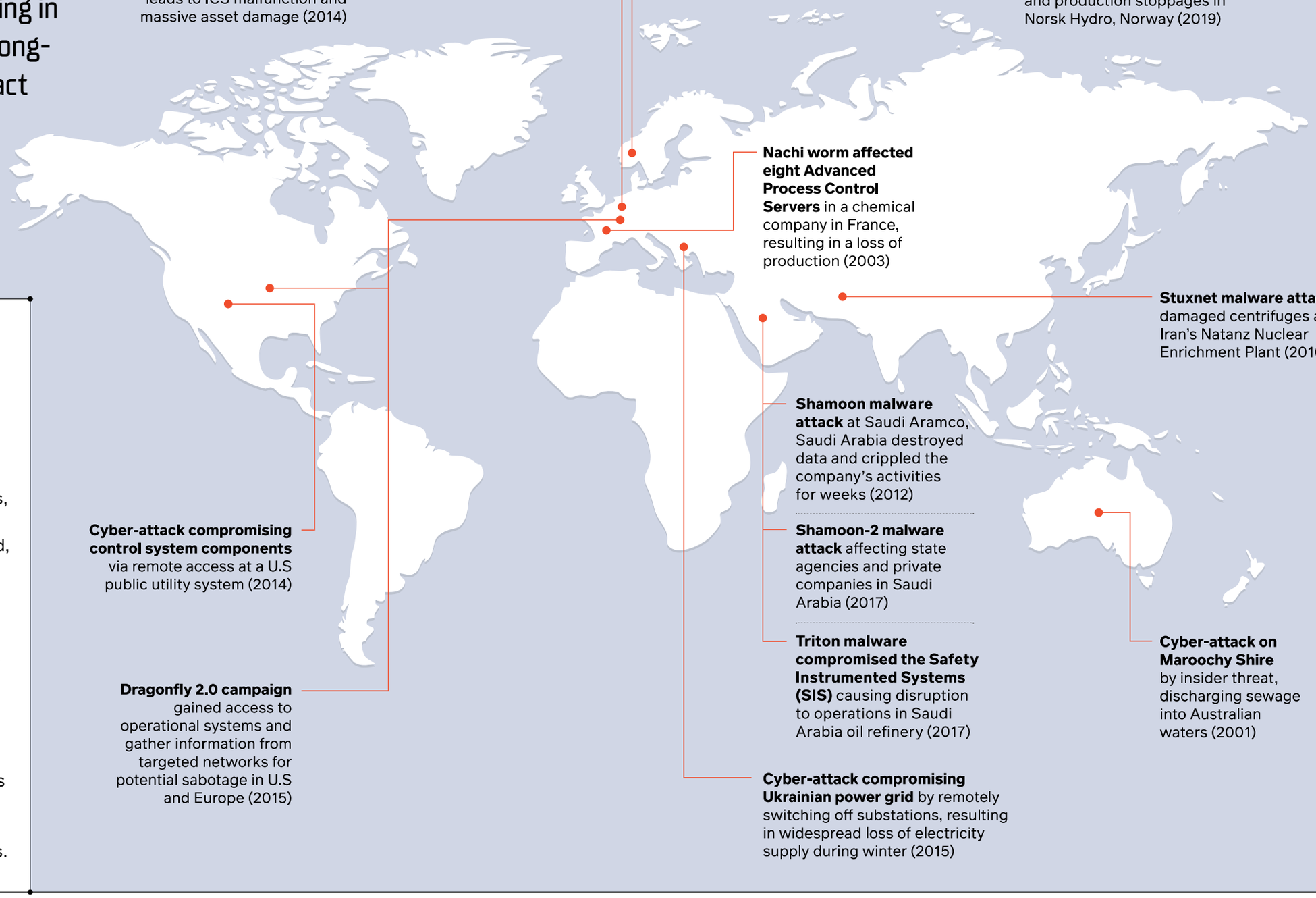
In the past, malicious cyber activities were limited to website defacement, data theft and cyber-fraud. Cyber criminals also relied on social engineering tactics – for example, through phishing emails that entice individuals to click on malicious links that will compromise their accounts or online credentials.

A more worrying threat has developed with the increased connectivity between IT and OT systems. Adversaries are now able to compromise IT systems connected to the Internet, secure their footholds, and move to the OT systems to disrupt industrial processes.

OVERVIEW OF CYBER-ATTACKS AGAINST OT SYSTEMS

Cyber-attacks against OT systems are increasing in number and having long-lasting and real impact

The malicious actors carrying out these cyber-attacks adopt vastly different modus operandi from the run-of-the-mill hacktivists or cybercrime groups. They are often sophisticated Advanced Persistent Threat (APT) groups, which are a class of cyber-attackers, typically state-linked, who can compromise systems and remain undetected for an extended period of time. They aim to conduct cyber campaigns to steal information or disrupt operations. Furthermore, the proliferation of smart technologies and the increased digitalisation of industrial system environments introduce a wider attack surface for APT groups to conduct their cyber campaigns.



Spear phishing and APT attack at German steel mill leads to ICS malfunction and massive asset damage (2014)

Ransomware attack caused a loss of access to customer orders and production stoppages in Norsk Hydro, Norway (2019)

Nachi worm affected eight Advanced Process Control Servers in a chemical company in France, resulting in a loss of production (2003)

Stuxnet malware attack damaged centrifuges at Iran's Natanz Nuclear Enrichment Plant (2010)

Shamoon malware attack at Saudi Aramco, Saudi Arabia destroyed data and crippled the company's activities for weeks (2012)

Shamoon-2 malware attack affecting state agencies and private companies in Saudi Arabia (2017)

Triton malware compromised the Safety Instrumented Systems (SIS) causing disruption to operations in Saudi Arabia oil refinery (2017)

Cyber-attack on Maroochy Shire by insider threat, discharging sewage into Australian waters (2001)

Cyber-attack compromising control system components via remote access at a U.S public utility system (2014)

Dragonfly 2.0 campaign gained access to operational systems and gather information from targeted networks for potential sabotage in U.S and Europe (2015)

Cyber-attack compromising Ukrainian power grid by remotely switching off substations, resulting in widespread loss of electricity supply during winter (2015)

HOW THESE GLOBAL OT CYBER TRENDS AFFECT SINGAPORE

Shinichi Yokohama
Chief Information Security Officer,
NTT Corporation,
Japanese telecommunications company

"World-wide, attacks that aim service sabotage at critical infrastructure such as a petroleum plant, an electricity utility, a nuclear power plant, are real. NTT estimates OT cyber threats will spread from critical infrastructure industries to other industries such as manufacturing. Awareness among business executives is just emerging, and NTT believes top-down action taking is critically important."

APT groups that carry out cyber-attacks are of grave concern globally. Singapore is not immune to this threat. As Singapore transforms itself into a Smart Nation – a hyper-connected country that deploys smart technologies to enhance the quality of life for every citizen – our livelihood and economy will increasingly depend upon and be impacted by the digital domain.

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. We need vigilance in safeguarding these systems toward ensuring a robust and resilient Smart Nation.

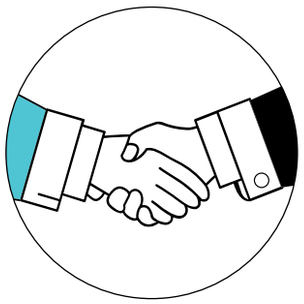
THE NEED FOR AN OT CYBERSECURITY MASTERPLAN

The Cyber Security Agency of Singapore (CSA) has developed the OT Cybersecurity Masterplan ('Masterplan'), as part of its continuous efforts to enhance the security and resilience of Singapore's essential service sectors, improve cross-sector response to mitigate cyber threats in the OT environment, and strengthen partnerships with industry and stakeholders.

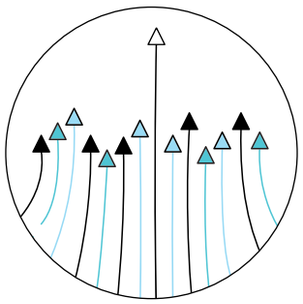
Lim Thian Chin
Director, Critical Information Infrastructure (CII), Cyber Security Agency of Singapore

"CII sectors delivering essential services are facing greater cyber threats today. There is a need to focus efforts on safeguarding CII sectors provisioning essential services. We hope that with the timely publication of the OT Cybersecurity Masterplan, it can drive efforts to address some of the people, process and technology challenges faced by CII sectors operating OT systems."

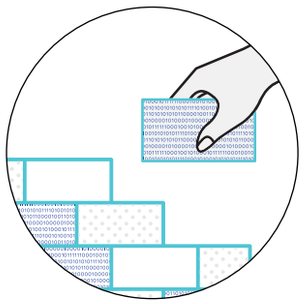
The Masterplan has the following objectives:



- Create awareness on the challenges faced by the OT stakeholders and promulgate cybersecurity solutions developed through Public-Private Partnerships.



- Align the efforts of multiple OT cybersecurity initiatives to address emerging cyber threats in the OT environment to better prevent, detect, respond and recover from cyber-attacks.



- Guide the development of key OT cybersecurity initiatives and build capabilities and competencies in securing the OT environment, in partnership with industry and stakeholders.

WHO THE MASTERPLAN IS FOR

The Masterplan is primarily relevant to the Critical Information Infrastructure (CII) owners who operate OT systems. The Masterplan underscores the need for a cohesive cybersecurity effort within and across sectors, as well as lays out key initiatives that will help CII stakeholders augment the cybersecurity of their OT systems.

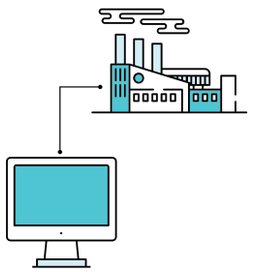
Notwithstanding, the Masterplan also applies to other enterprises running OT systems, which face the same OT threats and possess the same vulnerabilities. These include manufacturing plants in the oil and gas sector, semiconductor factories, and pharmaceutical companies, among others. Enterprises can leverage the capacity building mechanisms in the Masterplan to strengthen overall cyber resilience in their businesses.

In addition, the Masterplan will be useful for members of the OT cybersecurity industry, including equipment manufacturers, system integrators and penetration testers, to better understand OT cybersecurity challenges, and where feasible, develop products and technologies that can be used by owners or operators to strengthen the security of their OT systems.

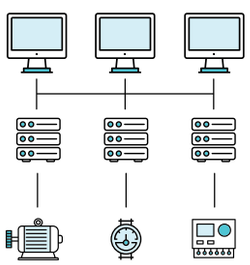
FOCUS AREA: INDUSTRIAL CONTROL SYSTEMS

The focus of this Masterplan is on Industrial Control Systems (ICS), as ICS makes up a majority of OT systems. ICS are industrial automation systems responsible for data acquisition, visualisation and control of industrial processes. They are deployed using different protocols configured to operate in various industries based on their specific operational needs. ICS communicate with field devices, such as electrical sensors and actuators that work together to monitor, control and achieve an industrial process objective. For example, Distributed Control Systems (DCS) are used in power stations to monitor and control turbine generators to generate electricity. DCSs are also used in water treatment plants to monitor and control the pumps and valves involved in the treatment of used water.

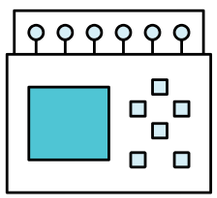
ICS include:



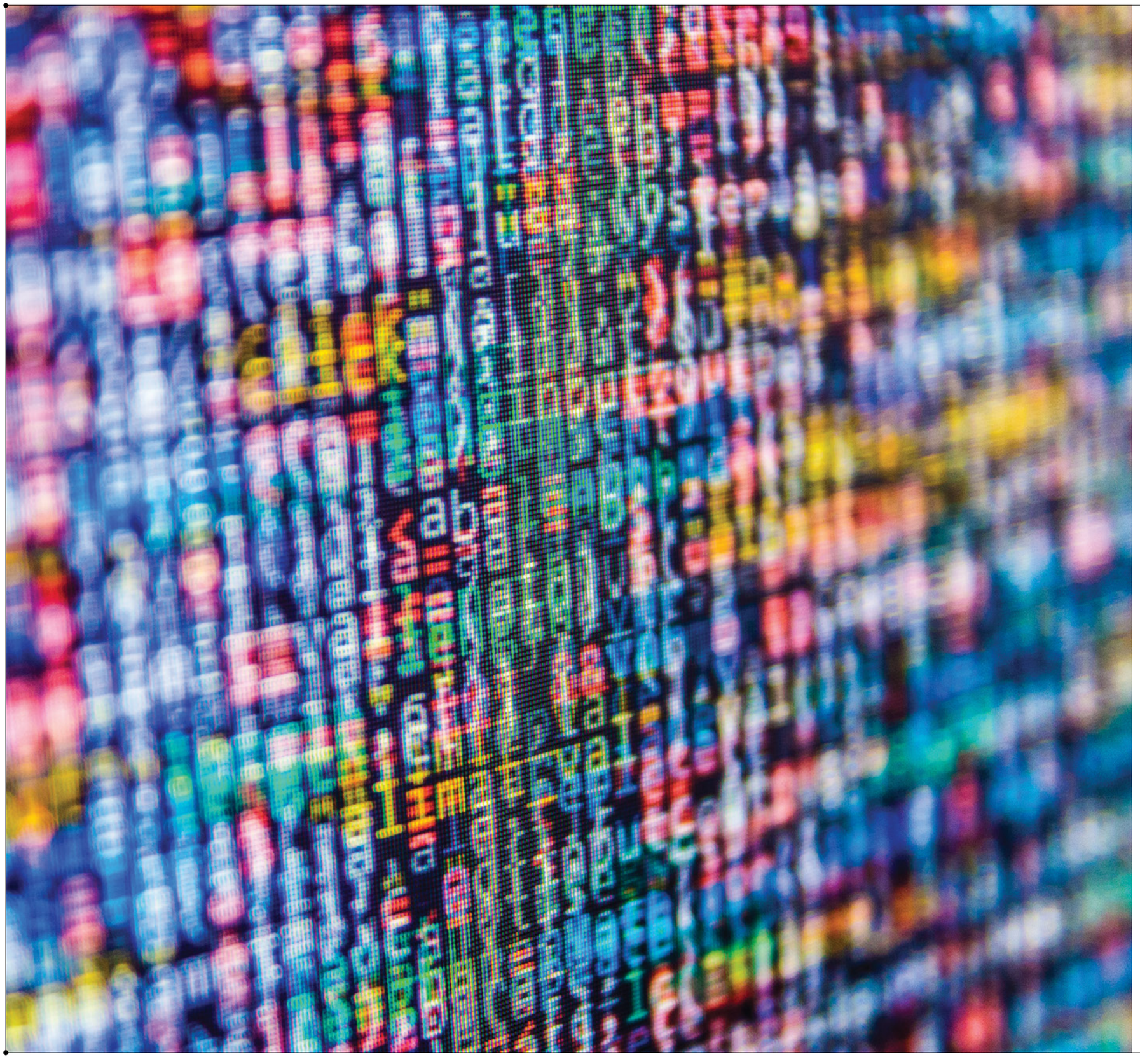
- Supervisory Control and Data Acquisition (SCADA) systems, which are typically geographically dispersed systems with long-range communications to monitor data and control industrial functions in remote locations.



- DCS, which are process oriented, closed-loop control systems with multiple controllers and integrated applications typically used within a single location, such as a manufacturing plant.



- Programmable Logic Controllers (PLC), which are singular controllers with discrete applications also functioning on closed-loop communication within a localised plant.



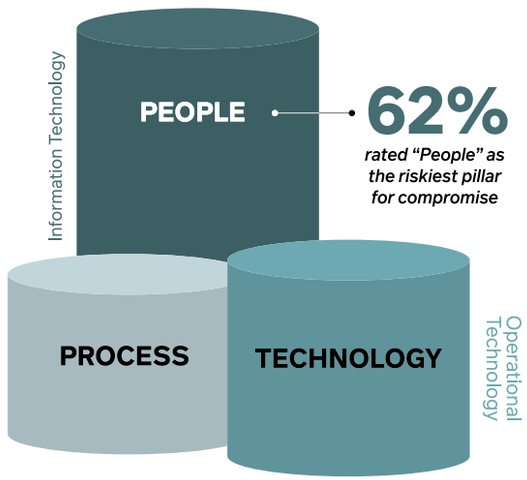
CHALLENGES TO SECURE ICS

ICS have become increasingly attractive targets for cyber-attacks primarily because successful attacks in the ICS environment can have significant consequences in the physical world. A notable example of an attack on ICS is the 2017 Triton malware attack in Saudi Arabia, where a critical infrastructure's Safety Instrumented System (SIS) was compromised by the malware, causing the safety controllers to enter 'fail safe' mode and shut down the industrial process. As a result, operations in nuclear, oil and gas plants were interrupted.

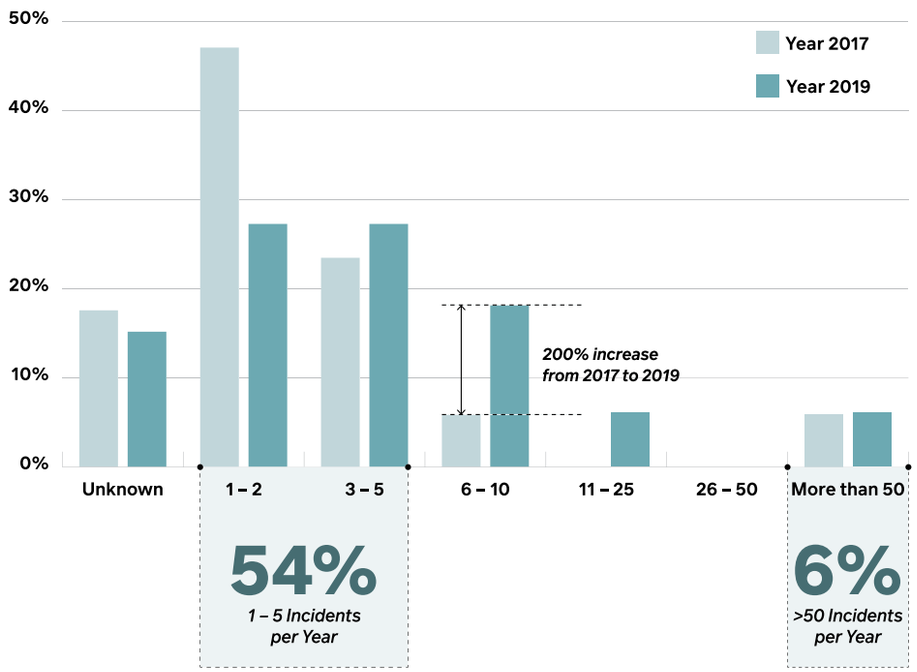
CHALLENGES TO SECURE ICS

SANS 2019 State of OT/ICS Cybersecurity Survey reported a general growth of ICS incidents in 2019 compared to 2017 – for example, there was a 200% increase in the number of organisations that reported between 6 to 10 ICS incidents within this time period. Among ICS components, SCADA and PLC were highlighted as having the highest impact to manufacturing and production processes. The survey also found that 62% of respondents considered people as the greatest risk for compromise to ICS, compared to 22% technology and 14% process. Organisations are encouraged to develop action plans on how their OT systems will operate with IT systems, as well as invest in external third-party cybersecurity assessments and establish a detailed inventory of assets.

Risk Categories for Compromise

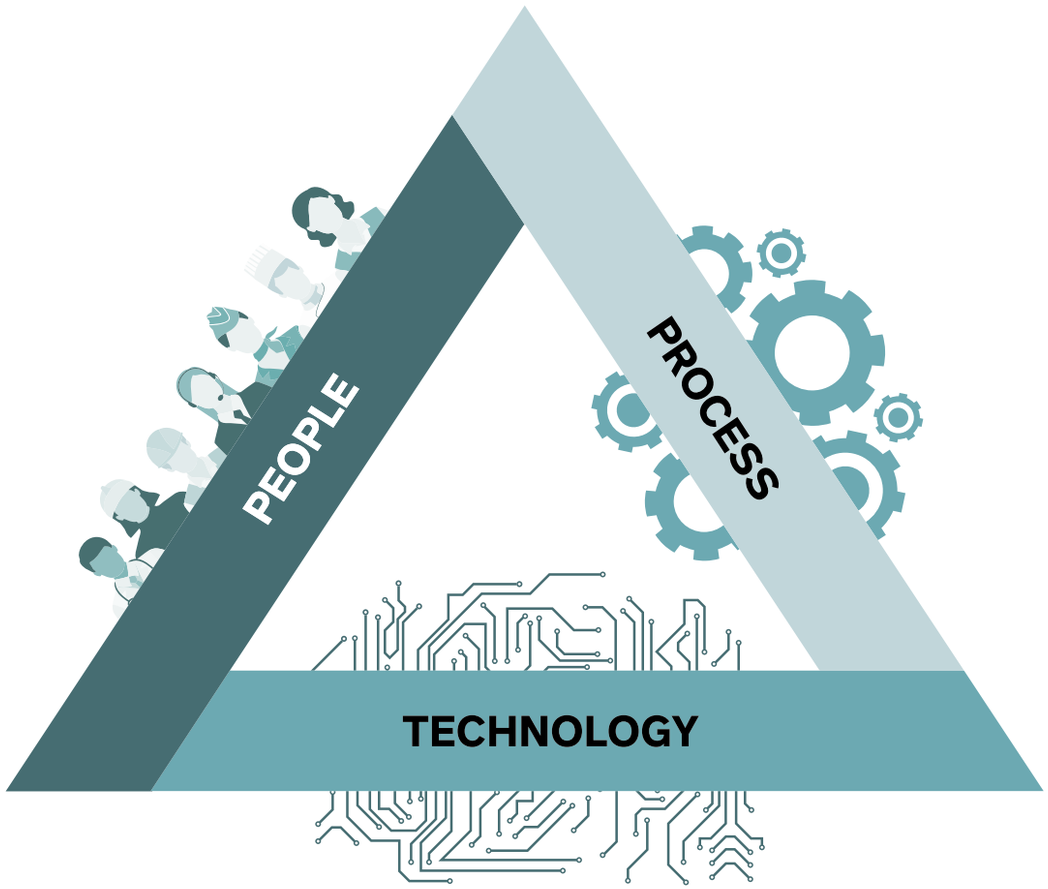


Number of Incidents in the Past 12 Months



Above infographics referenced from SANS 2019 State of OT/ICS Cybersecurity Survey

Trifecta of People, Process, and Technology



Stakeholders globally are facing challenges in securing their systems. The challenges in the OT environment can be grouped under the trifecta of people, process and technology, originating from the Diamond Model by architect Harold Leavitt in 1965, and subsequently popularised in the info-security community by cryptographer Bruce Schneier.

PEOPLE

To protect against external threats, more needs to be done beyond strengthening the network. There is a need to shift from the traditional mind-set that OT systems are isolated or within a closed network, and hence safe from cyber-attacks. A platform of trust and communication to facilitate information sharing among sectors and businesses is necessary to share actionable insights with other stakeholders for situational awareness, and to detect and respond to cyber threats promptly. There is also a need to consider third-party and supply chain compromises, which are fast becoming a realistic avenue of compromise for an attacker to gain a foothold into OT systems.

People are the key resource of any organisation. Engineers working on OT systems must be trained on cyber threats and its mitigating measures. There is often a disconnect between OT and IT engineers, as they have differing priorities. Firstly, ICS cybersecurity is typically managed by process (or OT) engineers – with little or no involvement from IT engineers – who are not prepared to share information openly due to market competitive pressures and information sensitivity. Secondly, process engineers prioritise the resumption of production, while IT engineers want to ensure that systems are fully secure before restarting production. These different priorities tend to impede operational response to cybersecurity incidents.

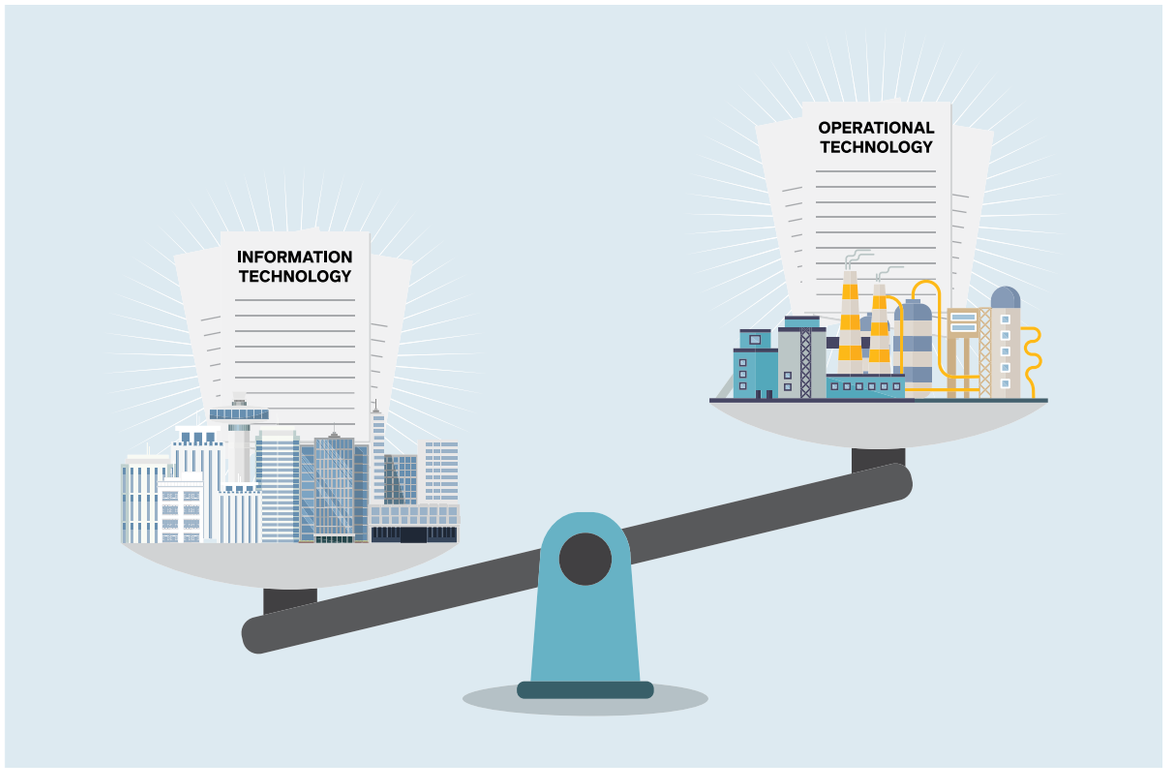
Therefore, the process engineers should work with IT engineers to understand that cyber threats can happen in their environment, and to put in place a suite of process and IT cybersecurity controls to better defend against external threats.

In order to effectively manage OT cybersecurity, the team of skilled defenders must comprise both engineers and IT analysts, covering the entire system cycle of cyber protection, threat detection, incident response and system recovery. This requires niche and targeted training for engineers and IT analysts to attain the necessary skillsets. There is therefore a compelling need to increase the numbers and skill levels of our OT cyber defenders.

David Foo
Senior Director, Operations Technology, Maritime and Port Authority of Singapore

"Building a Smart Port will require us to progressively integrate and unify IT and OT systems in order to exploit the benefits of digitalisation. Inadvertently, this provides new opportunities for cyber-attackers given that OT systems tend to be more vulnerable as they have traditionally been designed to be separated from IT systems. Any successful attack on individual OT or integrated IT-OT systems can cause major disruptions to port operations. Therefore, the integration of IT and OT cybersecurity strategies is critical to address such risks. As the maritime sector regulator for cybersecurity, MPA will partner CSA closely in implementing the OT Cybersecurity Masterplan to ensure that Singapore remains a safe, efficient and sustainable global hub port."

PROCESS



In order to bring people together in a coordinated manner and have a common understanding, organisations must have governing processes in the form of policies, standards, guidelines and procedures in place. At the top tier of formalised governance are policies, which provide a generalised overview of the organisation's security needs and direction. This is followed by mandatory codes and standards for compliance, as well as recommended guidelines for best practice. Finally, all of the above are distilled into procedures for detailed steps on the exact actions necessary to implement a specific mechanism, control or solution. Only through such formal documentation can organisations produce a robust and reliable security infrastructure by reducing uncertainty and simplifying complexity.

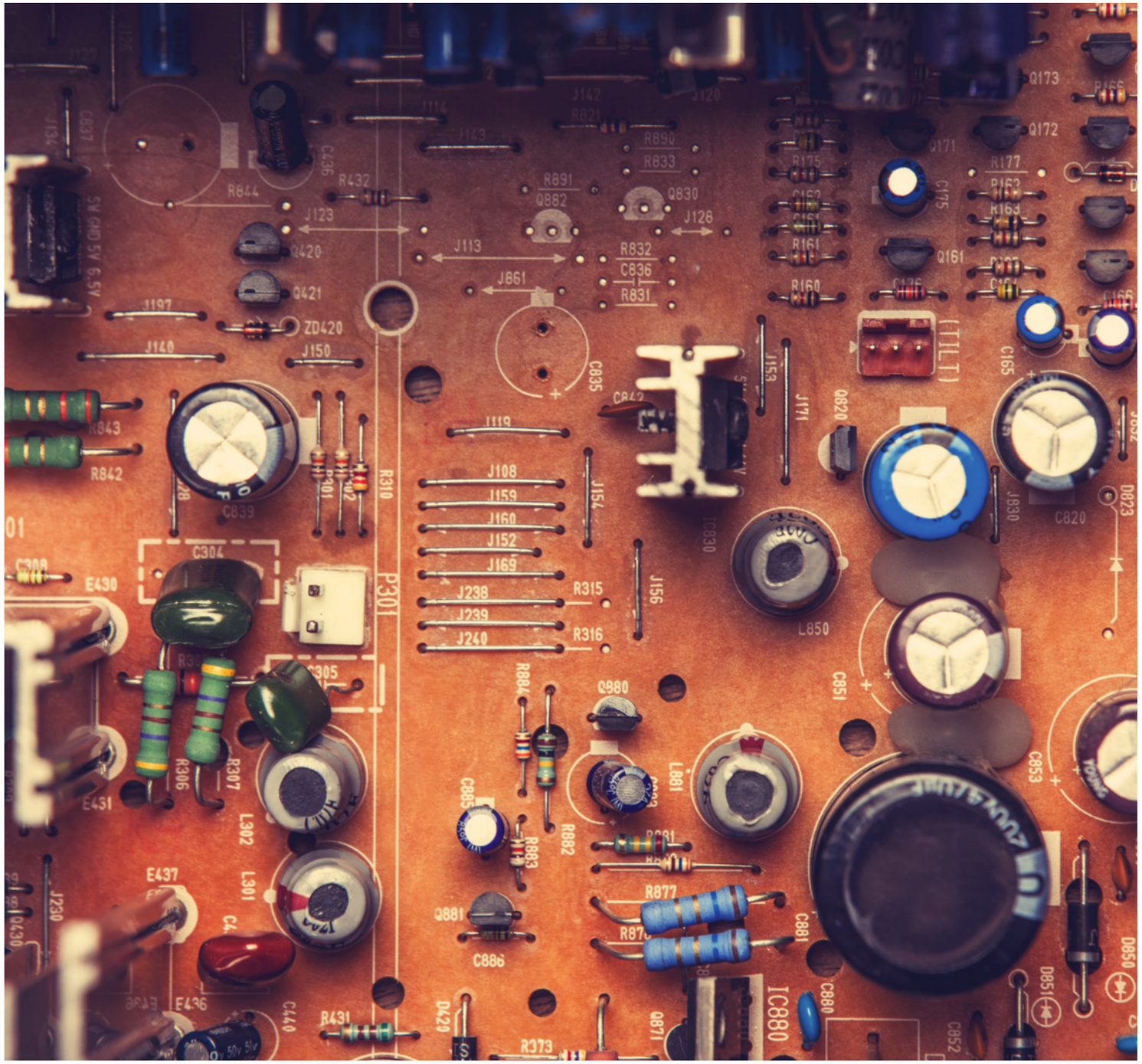
While there are established global OT cybersecurity standards and guidelines, what is lacking is a set of localised guidelines for OT stakeholders. Many attack vectors can make the jump from IT networks to OT systems, through the use of USB drivers for file transferring, an external contractor with an infected laptop performing maintenance, and even through a compromised software patch. Optimal ICS security can be achieved by strengthening the network, backed up with appropriate policies and procedures to prevent infiltration through these vectors. In addition, having prepared and practised response plans in case of an incident minimises damage to the assets.

Furthermore, ICS service support is often via a single proprietary vendor. Protocols and software codes are not shared with customers; while maintenance hooks, backdoors and other vulnerabilities are unknown to users. As a result, patching is irregular and only limited to ad-hoc hot-fixes when vulnerabilities are discovered. This leaves ICS operators at the mercy of malicious actors, who discover the vulnerabilities before they are patched and carry out zero-day attacks to compromise the system. To aggravate matters, in some instances, remote assistance through Virtual Private Network (VPN) connection into the system is required. If access is not controlled and authenticated properly, or if the link is not broken after maintenance, this serves as a conduit for malicious actors to exploit for entry into the system. There is a need for system owners to work with vendors to conduct regular code reviews, enhance patch management, and closely monitor remote access, which are process measures that help to better safeguard the cybersecurity of ICS. In addition, as systems become increasingly interconnected, more protocols are likely to become open source. This will mark a shift from the old philosophy of "security through obscurity" towards community threat hunting and vulnerability reduction.

Michelle Knight
GM, Industrial Control Systems, Shell, British-Dutch oil and gas company

"Shell has been on an ICS security journey for more than a decade. ***ICS security is one of the essential elements of ensuring asset integrity and preventing process safety incidents that could potentially result in harm to people or the environment. Safety is a deeply held value and we are committed to 'Goal Zero' - No Harm, No Leaks, because we care.*** *Partnering with CSA, allows for a unified country and industry approach to cyber security. This is aimed at raising awareness of the importance of cyber security, strengthening existing controls, as well as continuing to drive development of new process and technology to manage the ever-evolving threat environment we operate in."*

TECHNOLOGY

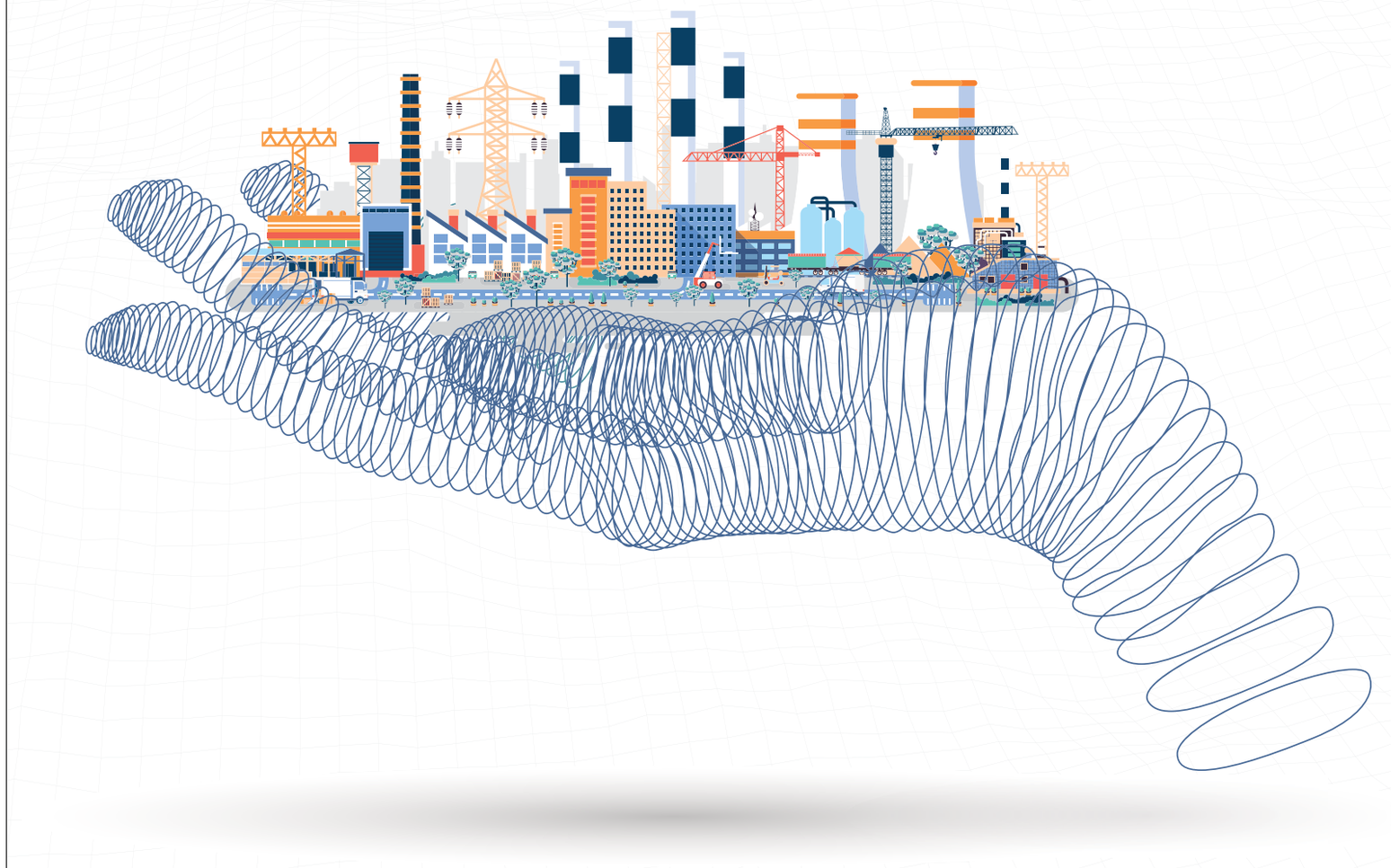


It is also vital that cybersecurity measures keep up with the rate of technology adoption. Legacy OT systems bring about unique cybersecurity challenges as these systems are often more prone to failure towards any modifications or changes (e.g. due to aging technologies) and they are usually run on obsolete software and hardware. There is also often a lack of basic cybersecurity controls, such as encryption and authentication, designed into legacy ICS systems. With legacy OT infrastructure, protecting these systems against cyber-attacks remains a challenge. This is made worse by the increasing demand for systems to be built at a faster pace, which often causes cybersecurity-by-design to be neglected. With more systems and devices being connected, it increases the attack surface creating an impetus to explore innovation cybersecurity solutions in the OT domains in order to better protect our systems and users.

In the current age of continuous and rapid evolution, the technological landscape is ever-changing. This especially applies to many cybersecurity aspects where new threats are emerging and new vulnerabilities are being discovered every day. Therefore, it is important that organisations stay abreast with technology developments and seek to have updated security measures that mitigate against the latest threats.

Owners and operators should adopt a “defence-in-depth” approach by implementing multiple technical or logical controls, physical controls and administrative controls to protect their assets. This way, even if one layer is breached, malicious actors are not able to access the organisation’s “crown-jewels” easily.

When designing defences, it is also important to note the inherent differences between IT and OT, which traditionally serves different purposes. IT environments are more dynamic and data centric while OT systems are more process centric and concerned with availability and safety. Therefore, designers of security systems must appreciate these priorities when building in cyber defences for ICS.



KEY THRUSTS

The OT Cybersecurity Masterplan outlines the key thrusts to uplift the cybersecurity posture of people, process and technology of OT stakeholders. Key thrusts include:

KEY THRUST 1: OT Cybersecurity Training

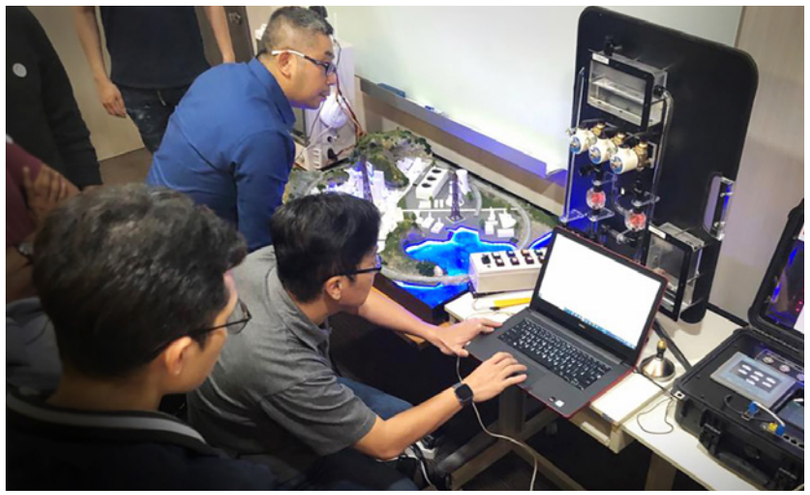
KEY THRUST 2: OT Cybersecurity Information Sharing and Analysis Center (OT-ISAC)

KEY THRUST 3: Strengthening Policies and Processes

KEY THRUST 4: Adopting Technologies for Cyber Resilience

OT CYBERSECURITY TRAINING

NSHC instructor explaining attack scenario with trainees.



Trainees performing an attack on the simulation model.

The CSA Academy was set up in September 2017 to raise the Government's and CII sectors' preparedness, response and resilience against cyber threats. It provides customised intermediate to advanced training courses in cybersecurity areas that are not readily available in the market. Courses offered by the CSA Academy cover different specialisations and technology platforms to address different threat actors and attack vectors, and offer realistic environments that trainees can relate to their day-to-day cybersecurity work. In 2018, FireEye became CSA's first training partner and delivered courses on incident response and malware analysis to CSA and other Government officers.

As part of the effort to build a more secure and resilient OT community, CSA Academy is rolling out OT cybersecurity courses to train between 70 to 100 OT cybersecurity professionals annually. The first OT cybersecurity course which focused on OT ethical hacking was launched in September 2019 in collaboration with NSHC Singapore, a security service company. The course equips participants with recent trends of different cyber-attacks on ICS facilities and OT cybersecurity ethical hacking skills, followed by measures to defend against these cyber-attacks. Due to the overwhelming demand, CSA Academy will be conducting another two runs in 2019.

CSA Academy is also working with iTrust, a Singapore University of Technology and Design (SUTD) R&D Centre, to launch an OT cybersecurity course. iTrust water and electrical testbeds and training skids will be used to provide a realistic training environment for OT cybersecurity incident response. The course will equip participants with best practices in securing OT systems via hands-on exercises and responding to realistic simulations of sophisticated cyber-attacks in the OT environment. In addition, the state-of-the-art testbeds and training skids from iTrust will facilitate research and training in the design of safe and secure OT systems.

Ng Joo Hee
Chief Executive,
Public Utilities Board,
Singapore's national water agency

"A properly functioning water system makes everyday life in Singapore possible, and is a basis of our continued prosperity. The threat of cyber-attacks on the water system has to be one of most serious. In this respect, the expertise that CSA provides is crucial to safeguarding cybersecurity in the water sector. PUB is fully supportive of CSA's effort in training and developing a cadre of cybersecurity practitioners to protect Singapore's OT ecosystem."

OT CYBERSECURITY INFORMATION SHARING AND ANALYSIS CENTER (OT-ISAC)

Typical process in OT-ISAC

1. Link in email instigates download of a file allowing OS access
2. A member notifies OT-ISAC of the campaign
3. OT-ISAC reviews and alerts the community
4. After examining campaign, OT-ISAC determines if wider distribution is warranted
5. OT-ISAC sends time-sensitive alerts to GRF network to warn partner sharing communities
6. Community members share additional technical data and sandbox results
7. OT-ISAC disseminates the additional intelligence
8. A day later, a community member that received the warning is targeted
9. Member had taken precautions due to OT-ISAC alert
10. 1.5 DAYS — From start to finish, incident lasts 1.5 days
11. Community alert sent less than an hour after member's submission
12. Sharing model is voluntary, trusted, and leverages a multi-industry sharing architecture

Credit: Global Resilience Federation: Strengthen Your Defense Strategy.

Donnie W. Wilburn
IT Risk Management Manager, ExxonMobil Global Services Company, American oil and gas company

"Cybersecurity incidents continue to grow in volume, complexity and impact across all industries. Similar to safety sharing, we believe cybersecurity information sharing is a key component to improving our industry's overall cybersecurity resilience. Industry partners can leverage this information and apply learnings across the business and the industrial control environment. Cybersecurity is such a broad and complex area that it takes effective collaboration across all business areas to stay ahead of threats."

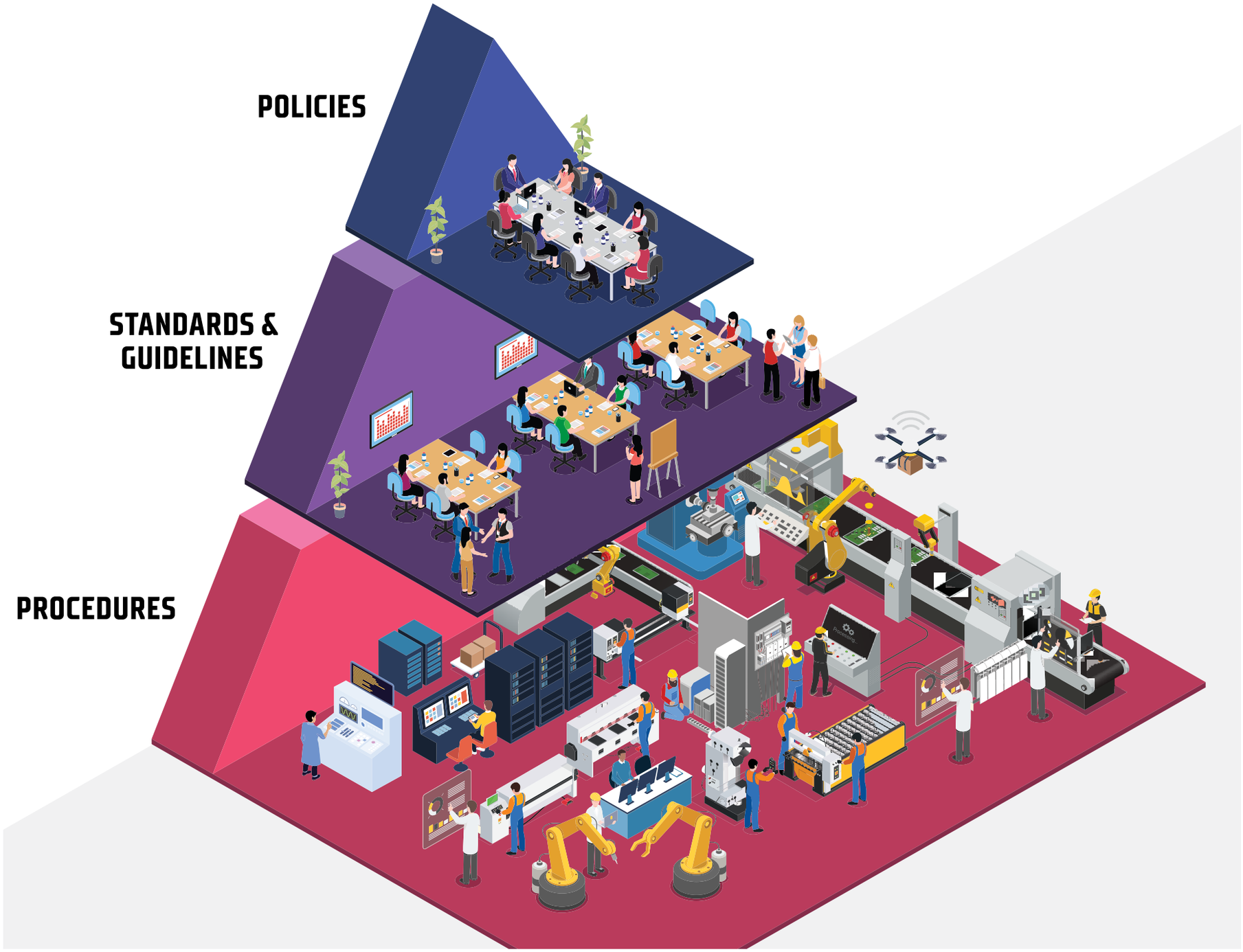
GRF APAC, a subsidiary of GRF, assists in the creation of member-driven information sharing and analysis centers (ISACs) for Asia Pacific regions or industries in need of a cyber, physical and geopolitical sharing community. GRF also provides support that augments analysis, technology, and operational capabilities for a community and its constituent members.

To enhance information sharing and permit timely responses against cyber threats, CSA collaborated with the Global Resilience Federation Asia Pacific (GRF APAC) and launched the OT Cybersecurity Information Sharing and Analysis Center (OT-ISAC) on 1st October 2019. The OT-ISAC will involve members from the Government, CII and OT industries, to drive knowledge exchanges and adoption of essential OT cybersecurity best practices and benchmarks. Through promoting conferences, workshops and meetings, OT cyber professionals can stay updated on fast-evolving threats and mitigation measures in the OT landscape. In addition, the OT-ISAC will offer insights from private cyber intelligence vendors on incidents that could directly impact the business operations of OT industries. The OT-ISAC will also tap on the experiences and expertise of more than 7,000 organisations operating across five continents, and share actionable cyber intelligence with OT cybersecurity stakeholders in Singapore.

The key objectives of setting up the OT-ISAC are to:

1. **Create a platform of trust,** to improve the willingness and confidence level for stakeholders to share knowledge, information and practices that could optimise cybersecurity outcomes.
2. **Tailor OT cyber information sharing for Singapore's needs.** With the establishment of the local ISAC, the usefulness and relevance of the shared information will be ensured.
3. **Build local OT cybersecurity analytics and response competencies.** The setup and the experiences of operating an ISAC provides opportunities to recruit, grow and deepen cybersecurity competencies of OT cybersecurity analysts for the local ecosystem.
4. **Foster cross-border cooperation on OT cybersecurity.** The setup of the OT-ISAC offers opportunities for the local OT industry to exchange information and partner regional countries to enhance collective cybersecurity.

STRENGTHENING POLICIES AND PROCESSES

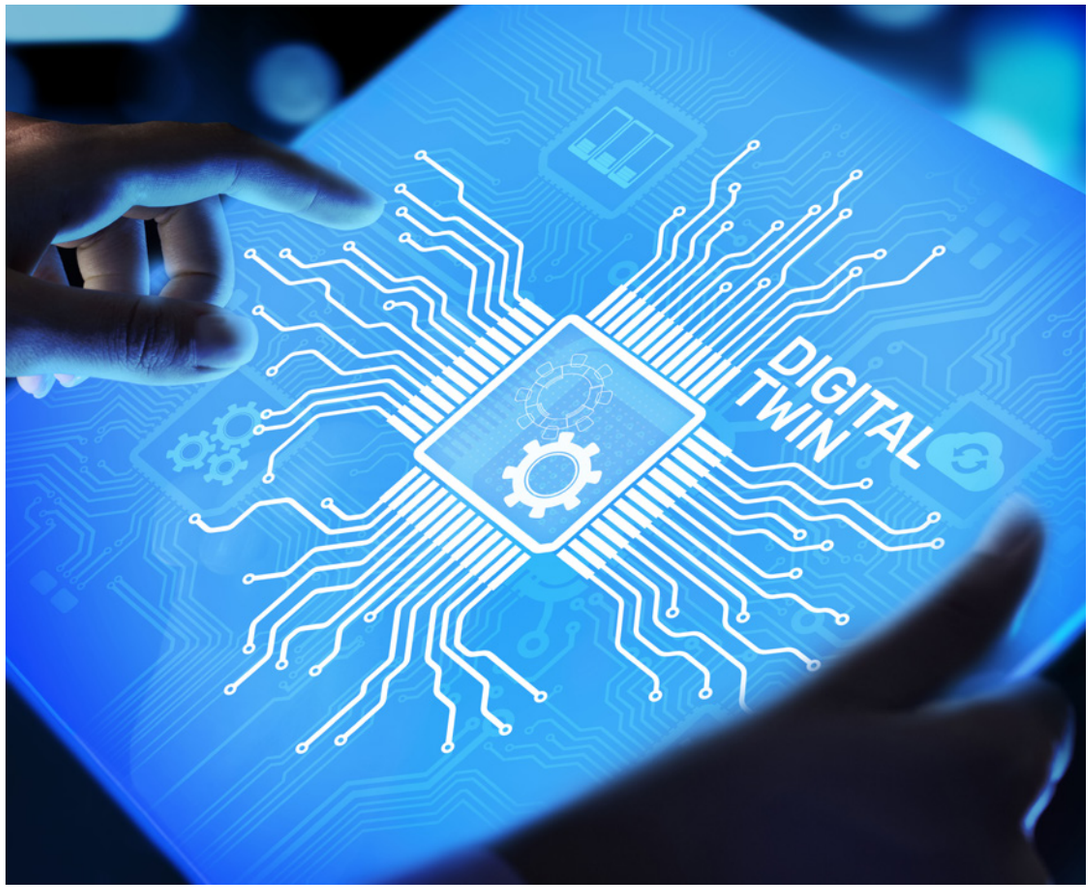


As part of the Cybersecurity Act that came into force in 2018, a Cybersecurity Code of Practice (CCoP) was issued by the Commissioner for Cybersecurity. The CCoP prescribes measures that owners of CII systems are required to implement, and mainly covers IT systems to date. CSA will augment the existing CCoP with a set of mandatory cybersecurity measures applicable to OT systems. This addendum is expected to be released in November 2019.

These measures provide cybersecurity controls and outcomes specific to OT systems, and focus on network segmentation, patch management, detection and continuous monitoring. They reduce the probability of threat actors exploiting software vulnerabilities and securing their footholds in OT systems, while helping to equip OT system owners with the ability to mitigate emerging cyber threats more effectively.

The measures included in the CCoP are modelled upon the ICS Cybersecurity Guidelines that CSA co-developed with the local ICS community, including OT CII owners. For businesses that own OT systems but which are not CII, these measures serve as best practices that they may wish to consider implementing.

ADOPTING TECHNOLOGIES FOR CYBER RESILIENCE



Mr David Koh (Chief Executive, CSA) second from left, interacting with the participants at Cybersecurity Innovation Day.

DEVELOPING INNOVATIVE CYBERSECURITY SOLUTIONS

To address the deficit in OT cybersecurity solutions, the Masterplan will push further for the development of innovative solutions within Singapore's OT industry. To help end users improve their cybersecurity posture and develop innovative cybersecurity solutions, CSA introduced the Co-innovation and Development Proof of Concept (POC) scheme in 2018 to support cyber innovation via seed funding to promising proposals and solutions.

The scheme grows Singapore's cyber industry by:

- ➜ Helping CII owners and participating user organisations improve their cybersecurity posture by tackling the cyber vulnerabilities faced;
- ➜ Providing opportunities for cybersecurity companies to develop new and innovative products and services; and
- ➜ Encouraging the trial and adoption of innovative solutions through partnerships between users and cybersecurity companies.

In September 2018, a pilot run of the industry call for innovation in collaboration with Ascendas-Singbridge, Energy Market Authority, PacificLight Power, Singapore LNG Corporation, Singapore Press Holdings and SMRT corporation attracted a total of 72 proposals, of which 8 proposals were successfully awarded funding. Projects funded include solutions leveraging Artificial Intelligence and Machine Learning to address OT cybersecurity challenges. Riding on the success of the pilot in 2018, the 2019 Cybersecurity Industry Call for Innovation will be launched at SICW 2019.

Nathalie Marcotte
SVP, Cybersecurity and Industry Services, Schneider Electric,
French energy management and automation company

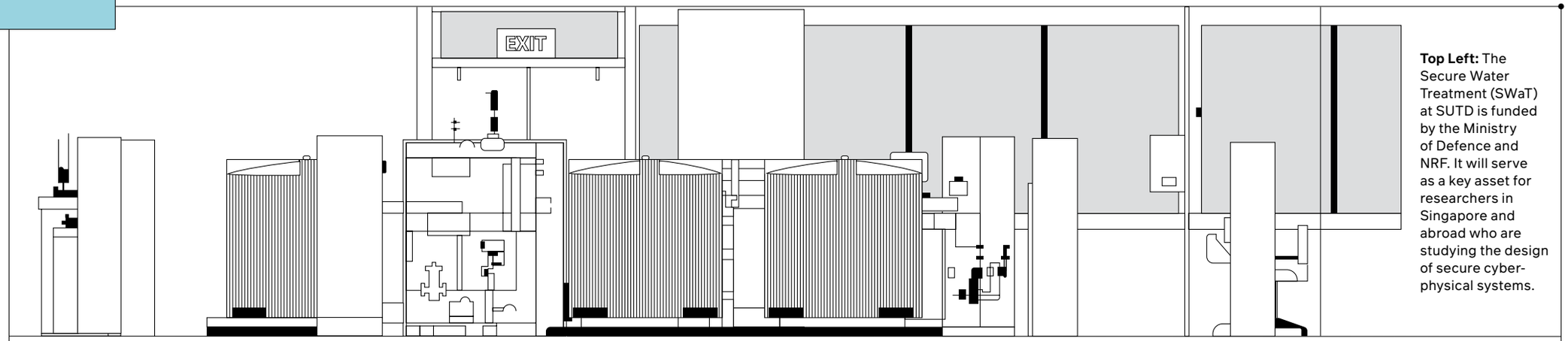
"CSA's Co-innovation and Development Proof of Concept (POC) Funding Scheme is another example of co-operation to leverage cybersecurity skills and technologies to develop innovative solutions that address key business priorities. Effective cybersecurity protection is only as strong as the weakest link. Schneider Electric believes in looking at cybersecurity across the operation and implementing solutions that consider the existing systems, as well as the potential value from future IIoT applications."

RESEARCH & DEVELOPMENT (R&D)

The National Cybersecurity R&D (NCR) Programme aims to improve the trustworthiness of cyber infrastructure with an emphasis on security, resiliency and usability. The NCR was launched in 2013 and received strong funding support of over $190M.

CSA has been working closely with the National Research Foundation (NRF) through the NCR Programme to develop advanced capabilities and cultivate innovative solutions to solve cybersecurity challenges faced by OT domains of which commercial solutions could not fully address.

Through the NCR, collaborations have been forged among the research community, industry and end users to address cybersecurity challenges in OT domains, developing local cybersecurity capabilities in the process.



Top Left: The Secure Water Treatment (SWaT) at SUTD is funded by the Ministry of Defence and NRF. It will serve as a key asset for researchers in Singapore and abroad who are studying the design of secure cyber-physical systems.

Middle: Secure Water Treatment (SWaT) overall process layout. Source: SUTD.

Bottom: Elevated reservoir tanks from the Water Distribution (WADI) test bed, extended from SWaT. Source: SUTD.

Projects funded by the NCR Programme span the cybersecurity challenges of asset identification, protection and threat detection of OT systems to strengthen its resilience. Some projects have demonstrated potential to be deployed in live environments and are ready for commercialisation.

- In the water sector, researchers have developed a prototype software tool to generate an inventory of OT assets – inclusive of field instrumentations – to better identify unauthorised OT devices connected to the network.
- In the land transport sector, researchers have developed a SCADA packet inspection firewall, a secure configuration management system and secure wireless communications mechanisms for its OT systems.
- In the water and energy sectors, prototypes to detect anomalous activities and formulate mitigation responses for OT systems were developed, based on machine learning technology.

The NCR Programme builds upon the research strengths developed in the local ecosystem, through the establishment of National Satellites of Excellence (NSoE). A NSoE on cyber-physical systems security has been set up at iTrust in SUTD. iTrust's research focuses on the development of advanced tools and methodologies to enhance the security and safety of current and future cyber-physical systems in three testbeds: the Secure Water Treatment (SWaT), Water Distribution System (WADI), and Electric Power and Intelligent Control (EPIC). In addition to supporting research, the testbeds are also used to validate commercial cyber intrusion detection systems and as training and exercise platforms for Government agencies, industry and students.

Hiroshi Tanoguchi
Head of Lifecycle Service Business Division, IA Systems & Service Business HQ, Yokogawa Electric Corporation, Japanese industrial automation company

"There is no perfect countermeasure in terms of cybersecurity protection, the cybersecurity managed service to monitor the ICS, to detect a malware or a malicious attack, to notify it to the customer and to take a quick action before having a serious incident is our key focus now."

OT CYBERSECURITY DETECTION AND MONITORING CAPABILITIES

A critical aspect of strengthening the OT cybersecurity posture in Singapore involves constant, robust monitoring of network activities within CII, and swift and decisive responses in the event anomalous activity is detected. This requires putting in place Security Operations Centres (SOCs) at the sectoral level to oversee, monitor and coordinate cybersecurity efforts between Government agencies and CII owners.

Mr Ngiam Shih Chun
Chief Executive, Energy Market Authority, Singapore's energy industry regulator

"The power system is a complex and critical network. With digitalisation and the rising trend of cyber threats, the Energy Market Authority will need to work closely with CSA to strengthen the reliability and resilience of our systems."

All CII sectors who operate OT systems are developing or have in place sectoral SOCs suited toward their respective operating environments, with three examples highlighted below:

- Since 2017, the Energy Market Authority (EMA) has collaborated with CSA on two systems to strengthen the cybersecurity of the power sector. This included a Sectoral Detection & Early Warning System (SDEWS) to detect cyber-attacks. The SDEWS analyses and monitors security logs sent from the power sector's CII for anomalous behaviour in the OT environment. Complementing this is the Cyber Threat Detection System (CTDS) that detects cyber anomalies in the OT network. These systems help EMA safeguard our power systems and ensure a reliable supply of electricity and gas for Singapore.

- The Maritime and Port Authority of Singapore (MPA) operationalised and officially launched the Maritime Cybersecurity Operations Centre (MSOC) in May 2019. The MSOC conducts round-the-clock detection, monitoring, and correlation and analysis of data activities across all maritime CII. This has helped to strengthen the maritime cybersecurity posture in Singapore against potential IT and OT cyber-attacks. Besides possessing the capability to detect and analyse anomalous activities and cyber threats in the IT environment, the MSOC is also able to respond to cybersecurity incidents by employing and integrating advanced OT technology solutions. In addition, MPA is in the process of linking the MSOC and the Port Operations Control Centre (POCC) to respond to cyber-physical incidents in a more holistic and timely manner.

- The Public Utilities Board (PUB) is also leveraging the expertise and infrastructure offered by the cybersecurity industry, and has subscribed to Managed Security Services for its SOC operations. This allows PUB to monitor and analyse its cybersecurity posture, as well as provide the cyber situational awareness and anticipate cyber threats. As part of PUB's capability development roadmap, it will also be harnessing new technologies to enhance cybersecurity resilience for the water sector.

CONCLUSION

This 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, evolving digitalisation and ease of conducting business-as-usual activities.

With cyber threats expected to become ever more sophisticated, it is vital for the Government, businesses and individuals to ensure that we have the right defences in place to protect our systems, detect and respond to breaches robustly in order to neutralise the threats expediently.

Given the niche expertise in OT cybersecurity, Singapore needs to grow our pool of cybersecurity professionals through continuous training and information sharing to deepen their competencies. Through this, we can build a stronger and more resilient cyber defence against the evolving cyber threats.

Our nation's resilience against cyber threats will also attract opportunities offered by new digital technologies that appeal to investors as a strategic and secure location for their business.

GLOSSARY

Term	Definition
Advanced Persistent Threat (APT)	An attack in which perpetrators successfully gain access to a targeted system and stay undetected for a long period of time to exfiltrate, modify, or destroy critical data. APTs can also refer to the advanced, and often state-linked or state-sponsored, threat actors that conduct extended campaigns such as cyber espionage.
Air-Gapped	Isolation of a system, at which there are no physical and logical interfaces connected to another system.
Digitalisation	The process of generating / converting analogue sources to a form that can be processed by a computer (digital format).
Hacktivists	An individual or group who wants to undermine the reputation or destabilise the operations of an entity, or to publicise their political or special agenda and again recognition, usually by hacking an organisation's website.
Information Technology (IT)	Arrangement of interconnected computers that is used in the storing, accessing, processing, analysing, and sending of information, e.g. computing and telecommunications equipment.
Operational Technology (OT)	Arrangement of interconnection computers that is used in the monitoring and/or control of physical processes, that includes: (a) Supervisory control and data acquisition systems, distributed control systems, and other control system configuration such as programmable logic controllers; (b) A combination of control components, e.g. electrical, mechanical, hydraulic, and pneumatic, that act together to achieve an industrial objective, e.g. manufacturing, transportation of matter, or energy.
Phishing / Spear Phishing	A common technique used by hackers to trick people (typically through emails) into divulging personal information, transferring money, or installing malware. Spear phishing is designed to be a more targeted approach.

Term	Definition
Ransomware	Malware that encrypts files on a victim's device, rendering them unusable until a ransom is paid, usually in the form of Bitcoin or other cryptocurrency. It may spread through phishing e-mails that contain malicious attachments or links, or malicious pop-ups that appear when users access unsafe websites.
Relay	An electromechanic component that controls an electrical circuit (open/close).
Safety Instrumented System (SIS)	A system that consists of an engineered set of hardware and software safety controls to provide fail-safe protection.
Social Engineering	A non-technical tactic hackers use to trick people into revealing sensitive information (e.g. passwords).
Supply Chain Compromises	An occurrence within the supply chain whereby an adversary maliciously tampered the system or the information to introduce security weaknesses that can be possibly exploited by the adversary during an attack.
Timers / Sequencers	A component that produces outputs based on variable timing or process sequence.
Virtual Private Network (VPN)	A data network that enables two or more parties to communicate securely across a public network by creating a private connection through authentication and encryption techniques.
Website Defacement	A malicious attack on a website that changes its visual appearance or content.

CONTACT INFORMATION

Cyber Security Agency of Singapore

Website:
www.csa.gov.sg

General enquiries/feedback:
contact@csa.gov.sg

Singapore's Operational Technology Cybersecurity Masterplan 2019

ISBN: 978-981-14-3668-0

Designed by:
APT811 Design & Innovation Agency
www.apt811.com