COALITION FOR CYBERSECURITY IN ASIA-PACIFIC

Cybersecurity Policy for Operational Technology:

A Guide for Governments

Executive Summary

Operational Technology (OT) is facing a growing threat environment. Cybercriminals and nation-state actors are successfully targeting and impacting critical infrastructure entities globally. With this increased scale of attack and threat surface, policies are needed to better secure industrial networks and their connected OT. This report seeks to help cybersecurity officials create an effective cybersecurity policy framework, and increase the resilience and security of these OT systems.

OT represents the collection of hardware and software that helps to monitor, manage, and control physical devices and their related functions and processes, including components such as valve controls at water treatment facilities, monitoring mechanisms at nuclear power plants, or robotics on manufacturing floors. OT comprises vital components within critical information infrastructure (CII)[1] sectors like utilities, and transportation systems. The role of government in ensuring CII and other sectors operate safely and securely naturally reflects an important and similar government role to ensure the cyber resilience of OT.

The importance of OT cyber-resiliency and the role for government is further underscored by the evolving cyber threat environment for OT, where the global trend of cyberattacks on OT systems has intensified and will only get worse. In a survey by Ponemon Institute, 90% of OT enterprise respondents reported suffering at least one damaging cyberattack between 2017 and 2019.[2] In sector-specific examples, cyberattacks on the maritime industry's OT systems have spiked by 900% over the last three years.[3] In a manufacturing example from June 2020, the SNAKE ransomware specifically targeted industrial control system (ICS) and supervisory control and data acquisition (SCADA) systems at Honda factories around the world, leading to production halts for several days. Digitization is also increasing and accelerated due to factors like COVID-19, which has only further raised the risks by increasing attack surfaces.[4]

Yet the governance landscape for OT within Asia is only in its early stages. Just 9 of 14 top economies in APAC have cybersecurity guidelines for OT protection, and only 4 out of 14 economies have policies in place to coordinate OT cybersecurity at the national or sectoral level. Current laws and policies typically focus on protecting enterprise IT systems within CIIs from cyberattacks. This is worrying as cybersecurity threats to OT systems mount, with OT enterprises in Asia suffering significant losses from cyberattacks, critical services and people's safety are being put at greater risk.

Countries need to address cybersecurity risks within OT. As such, governments should consider adopting policies to address OT cybersecurity that are risk-based and outcome-oriented, and allow enterprises and CII operators the flexibility to adopt the tools and technologies that are deemed appropriate and effective for their respective enterprises.

Governments can draw on emerging international and regional best practices and guidelines. These are still at a relatively nascent stage across Asia. Thus, governments have a unique opportunity to craft their respective national frameworks in ways that mutually support one another, both in terms of establishing regional norms that will improve OT cybersecurity and ensuring a level of regional consistency that allows companies and organizations that manage OT to scale their cybersecurity practices more uniformly as they operate and invest across the region.

1 Critical information infrastructures (CII) are ICT and OT systems that are deemed by the government as important for the continuous provision of essential services. Examples include telecommunications, water, electricity, food, finance, transport, etc. As they are essential to the day-to-day running of a country, governments will need to protect CIIs and establish a framework for oversight to ensure economic vitality and national security.

2 Ponemon Institute, March 2019, Cybersecurity in Operational Technology: 7 Insights You Need to Know. Available at: https://lookbook.tenable.com/ponemonotreport/ponemon-OT-report

3 Vanguard, July 2020, Maritime cyber attacks increase by 900% in three years. Available at: https://www.vanguardngr.com/2020/07/maritime-cyber-attacks-increase-by-900-in-three-years

4 In March 2020, Brno University Hospital, the Czech Republic's second-biggest hospital, had its operations crippled by a major cyberattack amid the COVID-19 pandemic. Surgeries were cancelled, operations were suspended, and the hospital had to transfer patients away. See Joel Khalili, 16 March 2020, Techradar, "Coronavirus hospital suspends activity over cyberattack". Available at: https://www.techradar.com/news/coronavirus-hospital-suspends-activity-over-cyberattack

Checklist for an Effective OT Cybersecurity Policy Regime

This report will highlight some use cases and advantages of OT, describe the cybersecurity risks involving OT, and provide recommendations adapted from global best practices to create an effective OT cybersecurity regime. These recommendations are compiled into a checklist for governments:

Institutional Foundations

- ☐ Identify and align with existing laws and regulations for cybersecurity in general
- ☐ Enable prosecution of cybercriminals by defining cyberattacks as illegal
- ☐ Create a mechanism for designating appropriate organizations as CII and appointing them with some cybersecurity responsibilities

National Strategy and Policy

- ☐ Develop, with the buy-in of OT stakeholders, a national cybersecurity strategy for OT
- ☐ Develop and publish OT cybersecurity guidelines for CII and non-CII operators, drawing from best practices and relevant international standards (both public and private); these may include requirements in areas such as:
  - Asset identification and management
  - Vulnerability and patch management
  - Logging, threat detection, and forensic analysis
  - Data modification restrictions
  - Network segmentation/ protection
  - Redundancy, business continuity planning, and disaster recovery
  - Local & remote access management
  - Response and containment
- ☐ Establish OT cybersecurity training and capacity building
- ☐ Establish cybersecurity information-sharing networks among sector-level oversight organizations, CIIs, and OT enterprises to establish a two-way reporting system, share cybersecurity knowledge, and coordinate efforts for rapid incident response and threat intelligence – such as an OT Information Sharing and Analysis Center (OT-ISAC)
- ☐ Promote OT cybersecurity innovation
- ☐ Develop voluntary certification frameworks that include OT, and frameworks for reporting OT cybersecurity incidents

Implementation

- ☐ Create OT cybersecurity risk assessment mechanisms for appropriate CII and OT systems with guidelines that are continually updated and reviewed
- ☐ Encourage non-CII OT operators to adopt cybersecurity guidelines voluntarily
- ☐ Use the public sector to lead by example
- ☐ Collaborate with other countries to share cybersecurity knowledge and threat intelligence

What is Operational Technology and What is its Importance?

OT is found in both the industrial and public sectors, and use cases vary widely. Many OT systems were designed as industrial control processes in an era when such systems were naturally separated from communications networks and a level of cybersecurity was achieved by the relative isolation of OT systems. Factors such as reliability and safety were more prominently considered then. More recent OT systems have some cybersecurity features built-in, but still lack the level of "security by design" inherent in information technology (IT) systems.

Some key OT categories and case examples include:

	Select examples	Essential services/CII examples
Building management	• Automated controls for heating • Ventilation or air conditioning within an office building or data center • Lifts	• When deployed in government and utility offices • Temperature controls in government data centers
Product Lifestyle Management (PLM)	• Software that automates administrative processes • Product development in a factory	• PLM systems for military systems and equipment • PLM systems for essential goods
Safety Automation	• Systems that detect and diagnose electrical problems for emergency stops • Proximity system to shutdown machines when a worker is near	• Safety systems for overheating in a power plant • Proximity detection on railway systems
Industrial Control Systems (ICS)	• Valve in a chemical factory that produces batches of materials according to a process control algorithm • Supervisory system to monitor factory processes	• Sewage treatment • Distributed control systems for oil and gas supplies
Smart City Systems	• Electric car management system • Smart lighting for streetlamps	• Traffic monitoring and management systems • Flood prevention systems
Transportation	• Baggage handling system • Cranes in ports	• Flight management system • Train signaling and control

Application of OT in a Traditional Manufacturing Enterprise's Network

Level 5 — **Enterprise Network**
Email, Intranet, etc.

Level 4 — **Site Business Planning and Logistics Network Management**
Business management, scheduling, strategic planning

Network segment / Industrial 'Demilitarized Zone'

Level 3 — **Site manufacturing Operations and Control Management**
Production control, operations management, remote access

Level 2 — **Supervisory Control**
SCADA, DCS, ICS

Level 1 — **Process Control**
Automation network, safety systems

Level 0 — **Physical Processes**
Sensors, machines, devices

Figure 1: Application of OT in a traditional manufacturing enterprise's network based on the Purdue Model[5]

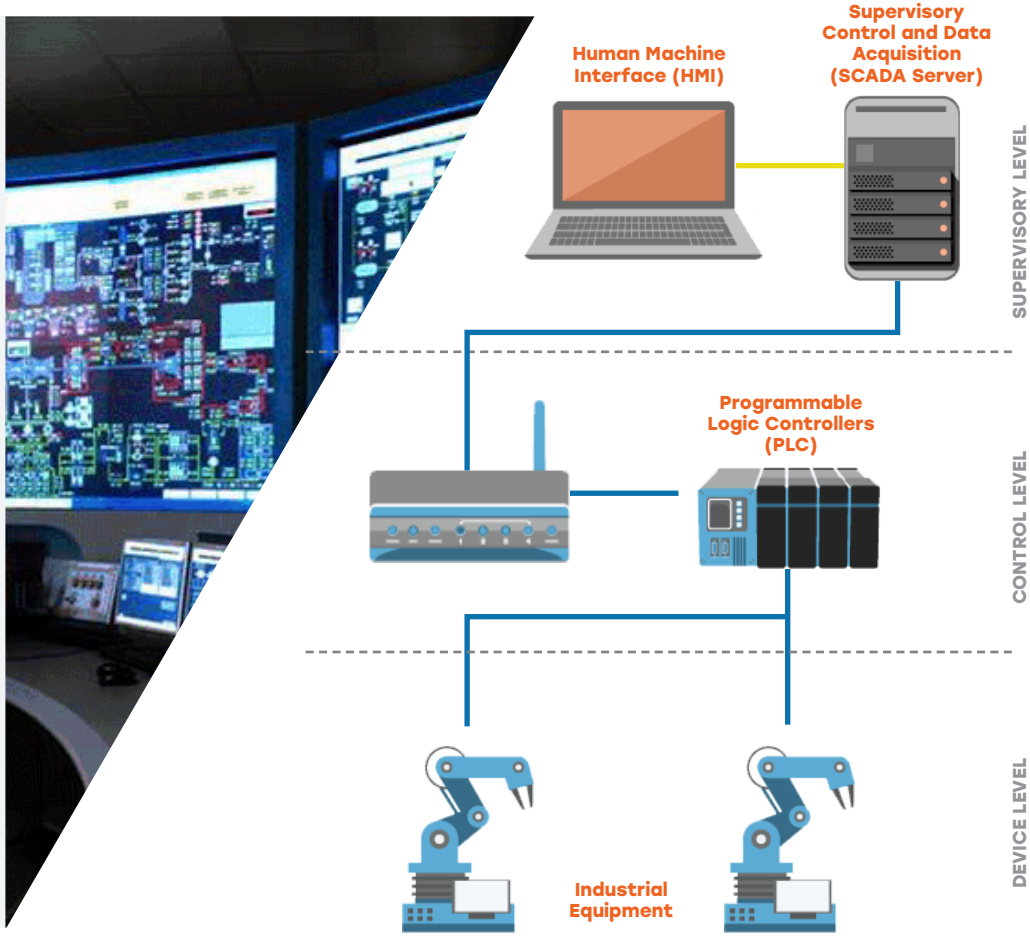


Figure 2: Diagram of an OT system that supervises factory processes[6]

5 Purdue Model adapted from https://owlcyberdefense.com/blog/how-iiot-and-the-cloud-are-upending-the-purdue-model-in-manufacturing

6 Diagram and picture adapted from https://medium.com/@Sp3ctreBlog/threats-to-operational-technology-and-the-vulnerabilities-to-scadadc684d595ea6

Today's rapid merging of IT/OT systems is attributable to the benefits of convergence such as:

- **Operational Efficiency –** Increased productivity arising from seamless, streamlined operations and implementation of new IT applications into OT environments.
- **Clarity –** Greater clarity to make smarter decisions from the use of real-time data insights.
- **Cost –** Converged IT/OT systems allow a single, integrated system to handle what was previously a complex system of multiple and diverse devices.
- **Safety –** Enhanced OT systems can identify potentially dangerous physical problems before they cause damage.
- **Agility –** IT/OT convergence allows for greater accuracy and speed in making operational decisions. The increased connectivity allows OT systems to adjust production according to data and supply/demand conditions, with multiple remote operations controllable from a central command center.
- **Cybersecurity –** Traditionally, OT cybersecurity was managed by the operations team due to the unique protocols and requirements of OT. However, the operations team specializes in operational matters, not cybersecurity. When managed correctly, smart OT cybersecurity products can be centrally controlled by the IT team, staffed with cybersecurity professionals who can strengthen the organization's overall cybersecurity posture.

Unfortunately, many OT systems today in Asia and elsewhere around the world lack adequate cybersecurity features and management. The growing convergence between OT and IT systems means that an attack either directly on OT or on OT-linked IT can have ripple effects on cyber risk across industries and broad national economic and security interests.

7 BBC, 22 December 2014, "Hack attack causes 'massive damage' at steel works ". Available at: https://www.bbc.com/news/technology-30575104

Why Attack OT?

OT cyberattacks, like those on IT, are driven both by cybercriminal organizations with economic motivations and nation-states with geopolitical or strategic motivations. Typical attacks include data theft, fraud, ransom, or disrupting the provision of key services in critical industries and sectors in order to disrupt economic or security interests of nation states. CII are prime targets for OT cyberattacks due to the importance of CII for economic and national security, and because attacks on CII can have a high impact, delivering the attacker strong "bang for the buck". Also, the increased connectivity and digitalization efforts in the OT environment has opened up more vectors of attack.

One example of a malicious attack on OT to disrupt critical infrastructures is the 2015 cyberattack on Ukraine's power grid. A malware named "Crashoverride" shut down one-fifth of Kyiv's total power capacity for an hour, affecting more than 225,000 consumers. In another example, a German steel mill was attacked, causing parts of the plant to fail which prevented the shutdown of a blast furnace and resulted in massive damage to the mill.[7]

Nation-state cyber actors as well as cyber criminals have successfully targeted and impacted numerous critical infrastructure entities in the past 5 years:

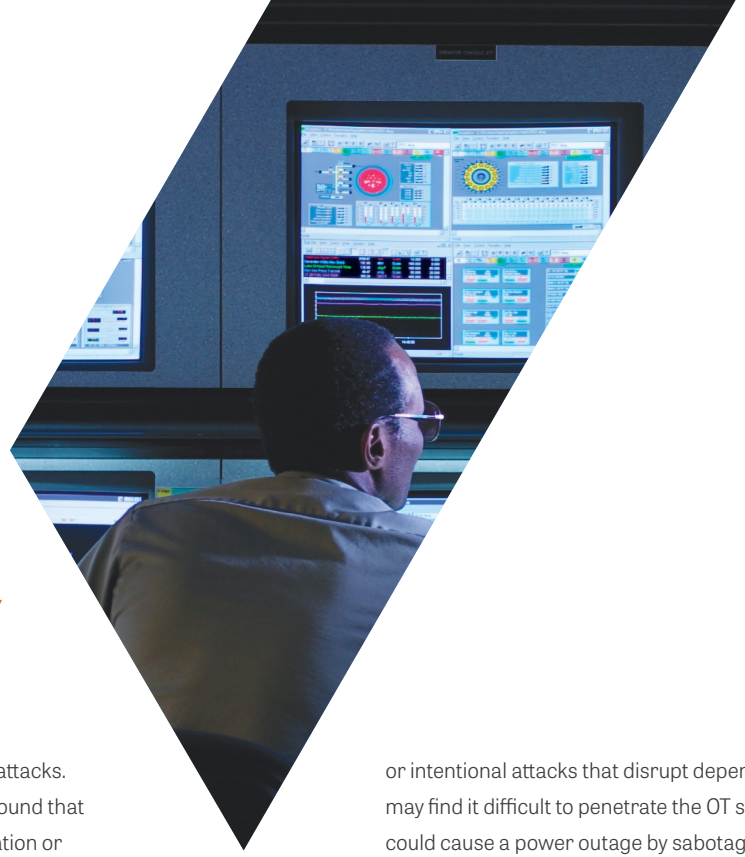
2015 Ukraine Power Grid – 225,000 homes no power

2016 Ukraine Power Grid – Industroyer/Crashoveride caused a 1-hour power loss

2017 Safety-instrumented systems for oil refineries - Targeted by Triton/Trisis

2019 US Oil & Gas - A natural gas compression facility was subject to a spearphishing attack to obtain initial access to the organization's IT network before pivoting to its OT for a ransomware attack, leading to a two-day shutdown

2020 Germany Hospital – The first ever death linked directly to a cyberattack occurred when ransomware disabled emergency care systems at a hospital. The hospital could no longer provide the critical care that the patient needed and the patient died after being diverted to another hospital 30 km away.



Increasing Vulnerability of OT to Cyberattacks

OT, especially in critical infrastructure, is an increasingly popular target for cyberattacks. A 2019 study by Siemens on cyber risk and cyber capabilities in the utility sector found that 56% of responders reported at least one attack involving a loss of private information or outage over 12 months. Yet, only 42% rated their cybersecurity readiness as 'high'.[8]

The impact of threats to OT are different from threats to IT systems. While cyberattacks to IT may result in compromise to confidentiality, integrity, and availability of data and IT functions, cyberattacks to OT may result in harms to safety, reliability, and productivity of workers and physical assets, as well as wider harms to the environment and broader sectors of economic activity.

The vectors of attack on OT systems may be external, such as supply chain attacks through infiltration of OT through an outside partner or provider, or more traditional online attacks from external sources. OT attacks may also be driven from within, through intentional misconfigurations, upgrade disruptions, incompatible cybersecurity measures, or intentional attacks that disrupt dependencies of OT systems. For example, an attacker may find it difficult to penetrate the OT systems of a power plant that is manned 24/7, but could cause a power outage by sabotaging the sub-station on which the OT system relies as such a sub-station may be unattended. Ultimately, attacks can be expected to come from anywhere throughout the network. OT vulnerabilities can be grouped into a few key categories, and are described in the following section under the well-known "People, Process, and Technology" Trifecta Framework, that identify the core elements cybersecurity programs should address.[9]

While some of these vulnerabilities described are common to any system, OT is especially vulnerable to threats related to "lock-in" from legacy systems and unique weaknesses related to the convergence of software and IT with physical OT platforms. Additionally, the overall impact of cybersecurity breaches for OT can be much more severe – including potentially loss of life given the physicality of these systems – and thus warrant greater attention from governments.

8 Joint study by Siemens and Ponemon Institute, 4 October 2019. "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?" Available at: https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf

9 RSA, 21 Jan 2016. "Securing the Digital World Part 3: Fundamentals of the Game - People, Process and Technology Alignment". Available at: https://www.rsa.com/en-us/blog/2016-01/part-3-fundamentals-of-the-game-people-process-and-technology-alignment
Eric Hess, Helical, 23 October 2019, "People, Process, and Technology: The Trifecta of Cybersecurity Programs". Available at: https://helical-inc.com/blog/people-process-and-technology-the-trifecta-of-cybersecurity-program

Risk categories include:

People

- **Enterprise staff may lack the proper skills to manage converged OT systems.**
  In converged OT systems, OT and IT teams need to understand the concerns and functions of each other, collaborating to balance cybersecurity needs with operational requirements.[10]

- **Enterprise staff may intentionally or unintentionally compromise OT systems.**
  Unintentional cybersecurity threats by staff may arise from a poor understanding of cyber risks and lack of cyber hygiene, which in turn lead to an increase in risk of OT incidents. Intentional sabotage of OT through an insider attack (such as a disgruntled employee acting alone or in concert with malicious actors) are equally problematic. Either way, people are often considered the weakest link in OT cybersecurity.[11]

Technology

- **OT devices are becoming 'smarter'.**
  OT systems have also become more advanced, increasingly connected to IT infrastructure, and are less constrained by point-to-point, closed systems. This allows for greater synergies between the enterprise's data system and business operations, becoming "smarter" with more sophisticated software and interconnectivity. However, they can be exposed to the same sophisticated threats that plague IT, such as cyberattacks and malware. That is, OT devices may have an increased attack surface due to software vulnerabilities or poor access configuration.

- **Older OT protocols have known cybersecurity weaknesses.**
  OT systems were designed for their specific industrial purposes and many were not designed with cybersecurity in mind. Cyber attackers may easily target systems through such vulnerabilities if enterprises fail to harden them.[12]

Process (planning, governance, operations)

- **Lack of investment and consideration for cybersecurity.**
  Cybersecurity investments may be difficult to justify in less mature organizations; both those focused on OT and connected to OT. This is often driven by short-term thinking or a lack of cybersecurity considerations in the strategic planning processes. The risk may be especially acute if or when organizations digitize (such as during the current COVID-driven phase of digitization) but focus only on the benefits and fail to manage the risks. In these cases, cybersecurity implementations for OT may lack sufficient resources or be neglected.

- **Use of outdated systems due to 'lock-in'.**
  OT systems often represent large capital investment and, as such, may have a lifetime much longer than development support for the software code base (thus losing key elements such as vulnerability patching support). For example, some legacy systems still run Windows 95 without a supportable option to upgrade a replacement or can only do so at high cost. Without enterprise lifecycle procedures to ensure that OT systems are regularly upgraded or replaced, enterprises are "locked-in" to outdated systems.

10 General Electric, May 2017. "An Executive Guide to Cyber Security for Operational Technology". Available at: https://www.ge.com/fr/sites/www.ge.com.fr/files/an-executive-guide-to-cyber-security-foroperational-technology-whitepaper.pdf ; and Security Boulevard, 10 December 2019. "Cybersecurity for Building Automation Systems". Available at: https://securityboulevard.com/2019/12/cybersecurity-for-building-automation-systems

11 Warwick Ashford, ComputerWeekly.com, 12 June 2019, "Operational technology security improving, but attack surface continues to grow". Available at: https://www.computerweekly.com/news/252464954/Operational-technology-security-improving-but-attack-surfacecontinues- to-grow

12 Derek R. Harp & Bengt Gregory-Brown, NexDefense, "IT/OT Convergence: Briding the Divide". Available at: https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf

Developing an OT Cybersecurity Regime

Policies and laws are needed to ensure that infrastructure, especially that which is deemed critical, is adequately protected, irrespective of the maturity, size or priorities of the operator. Both CII and non-CII systems will benefit from best practices developed and promoted by governments to enhance OT cybersecurity.

Current laws and policies typically focus on protecting enterprise IT systems within CIIs from cyberattacks. To address cybersecurity risks within OT systems, a country's cyber governance regime will need to address and include cybersecurity controls and outcomes specific to OT systems. As it stands today for many countries in Asia and around the world, existing regulations do not sufficiently cover OT cybersecurity concerns.

OT-specific policy can be developed to fill in the policy gaps and a checklist can support governments in this endeavour. The checklist proposed here is grouped into three stages: i) institutional foundations, ii) national strategy and policy, and iii) implementation. An analysis of the checklist items, along with country case studies and sources for the recommendations, are provided as follows.

#1 Institutional Foundations

Measures to be taken before an OT policy is created

- Identify and align with existing laws and regulations for cybersecurity in general
- Enable prosecution of cybercriminals by defining cyberattacks as illegal
- Create a mechanism for designating appropriate organizations as CII, and appointing them with some cybersecurity responsibilities

First, before implementing an OT policy, a legal basis for cybersecurity needs to be established. This can be done by enacting a general cybersecurity law for the country, such as Singapore's Cybersecurity Act[13] or Japan's Basic Act on Cybersecurity.[14] The cybersecurity law sets the nation's cybersecurity approach, establishes the responsible governmental cybersecurity agency (or commission) to have national cybersecurity oversight, and defines the responsibilities of government entities. Most countries have this in some measure at present – such as provisions to criminalize cyberattacks[15] and enable law enforcement agencies to conduct investigations and prosecute cyber attackers. But other elements are important for OT, such as providing the cybersecurity agency with the power and responsibility to designate the appropriate entities or functions as CII and to establish the cybersecurity requirements for those designated CIIs. Given the prevalence of ransomware attacks on both IT and OT, policies should be in place to punish and discourage such attacks, particularly by making ransomware payments illegal by any party. Rules to enable cyber insurance in line with emerging best practices are also important.

To help countries develop institutional foundations to protect CIIs, the Organization for Economic Cooperation and Development (OECD) recommends that such policies should also be developed in partnership with the private sector to help gain commitment from all stakeholders.[16] OECD also recommends governments demonstrate leadership by adopting clear policies, operating with transparency, and identifying which government agencies are responsible for CIIs.[17] These baseline foundations set the stage for a more robust national OT strategy and policy.

13 Cybersecurity Act 2018, Available at: https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312

14 The Basic Act on Cybersecurity. Available at: http://www.japaneselawtranslation.go.jp/law/detail/?ft=5&re=02&dn=1&gn=4&sy=&ht=A&no=104&x=0&y=0&ia=03&ja=04&ky=&page=3

15 Singapore's Computer Misuse Act establishes that it is an offence to intend, commit, or aid in unauthorized access or modification of computer material. Singapore's Computer Misuse Act is available at https://sso.agc.gov.sg/Act/CMA1993

16 OECD, 2008, "OECD Recommendation of the Council on the Protection of Critical Information Infrastructures". Available at: http://www.oecd.org/sti/40825404.pdf

17 OECD, 2008, "OECD Recommendation of the Council on the Protection of Critical Information Infrastructures". Available at: http://www.oecd.org/sti/40825404.pdf

#2 National Strategy and Policy

Steps to establish OT policy itself

- Develop, with the participation of OT stakeholders, a national cybersecurity strategy for OT
- Develop and publish OT cybersecurity guidelines for risk management by CII and non-CII operators, drawing from best practices and relevant international standards (both public and private); these may include requirements in areas such as:
  - Asset identification and management
  - Vulnerability and patch management
  - Logging, threat detection, and forensic analysis
  - Data modification restrictions
  - Network segmentation/protection
  - Redundancy, business continuity planning, and disaster recovery
  - Local & remote access management
  - Response and containment
- Establish OT training and capacity building
- Establish cybersecurity information-sharing networks among sector-level oversight organizations, CIIs, and OT enterprises to establish a two-way reporting system, share cybersecurity knowledge, and coordinate efforts for rapid incident response and threat intelligence – such as an OT Information Sharing and Analysis Center (OT-ISAC)
- Promote OT cybersecurity innovation
- Develop voluntary certification frameworks that include OT, and frameworks for reporting OT cybersecurity incidents

These steps focus on developing the OT cybersecurity regime by establishing an overarching strategy for OT through consultations and input from stakeholders in the country. The OT strategy sets the approach and actions that the country will take to build its cybersecurity regime around OT. Getting stakeholder input is important as it allows clarity about the needs and concerns of stakeholders as well as access to existing expertise in finetuning the policy. As technologies and cybersecurity are dynamic and rapidly changing, the government should work together with stakeholders to actively update the policy and help maintain the cybersecurity regime.

Consultation and discussion with stakeholders are also important to help draft standards and policies that are practical and not onerous. Variations in cyber governance and compliance requirements across countries and sectors can result in companies focusing on compliance instead of protecting their systems. Overly prescriptive cybersecurity regulations may not benefit organizations as cybersecurity has to be tailored to the risks and needs of the organization. Moreover, the existing global shortage of talent[18] means that cybersecurity teams are understaffed to deal with cyber risks in their IT systems, let alone OT systems. It is thus important that regulators ensure that any additional policies addressing OT cyber risks do not place undue compliance burden on stakeholders through consultations and dialogue.

One method to build and strengthen partnerships with stakeholders is to provide grants or other resources for organizations to conduct OT cybersecurity education and training for employees. In organizations integrating their IT and OT teams, this training of employees is essential to help employees manage the new converged system, but is sometimes overlooked.[19] In turn, the training will build up the capacity for IT/OT teams in the organizations to contribute and participate in further developing the cybersecurity regime.

Because of the diversity of OT systems, in general, successful OT cybersecurity regimes focus on risk management. Critical or high-risk systems face different challenges and have different needs than a general OT environment, even within the same organization. Similarly, OT may operate within very diverse contexts, some of which are highly static and predictable while

18 Wesley Simpson, Brink News, 4 December 2019, "A Global Shortage of Cybersecurity Professionals Leaves Businesses at Risk". Available at: https://www.brinknews.com/a-global-shortage-of-cybersecurity-professionals-leaves-businesses-at-risk

19 Damiano Bolzoni, Forescout, 11 July 2019, "3 pillars for a successful IT-OT cybersecurity strategy". https://www.forescout.com/company/blog/3-pillars-for-successful-it-ot-cybersecurity-strategy

others are more variable. Based on potential impacts, operators of some systems should be required or encouraged to ensure higher standards of protection than others, while having the flexibility to select the types of controls that are most appropriate for their contexts.

Below are three, regionally-diverse examples from Asia, America, and Europe that highlight various government approaches to cybersecurity policy for OT, with an analysis of the relevant policy elements and examples that might be considered by an authority seeking to establish or improve its regime. In addition to these regional governmental examples, a range of private sector initiatives on OT are also included to provide additional examples for governments to draw on as they craft an OT regime following the checklist above.

A national OT cybersecurity strategy: Singapore operational technology cybersecurity masterplan

Singapore's OT Cybersecurity Masterplan, one of the first in the world specific to OT, was published in 2019 to enhance cybersecurity and resilience among Singapore CIIs and other OT enterprises.[20] The Masterplan contains four key elements to heighten the cybersecurity regime: training and capacity building, developing a national threat information sharing and mitigation mechanism, updating existing cybersecurity policy to match new requirements, and promoting innovation through public-private partnerships.

With a focus on industrial control systems (ICS), the Masterplan's four key thrusts are:

1. **OT cybersecurity training to develop human capabilities:** The CSA Academy, established in 2017, will roll 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.

2. **Creating and facilitating the sharing of information through an OT Cybersecurity Information Sharing and Analysis Centre (OT-ISAC):** 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. The OT-ISAC will also tap into the experience and expertise of more than 7,000 organizations across five continents to share actionable cyber intelligence among OT cybersecurity stakeholders in Singapore. It will also facilitate information sharing with other countries.

3. **Strengthening OT owners' policies and processes through the issuance of an OT Cybersecurity Code of Practice (CCoP):** 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 covering only IT systems. As of December 2019, the CCoP has been updated to include OT systems – mandating certain OT requirements for CII and offering voluntary guidelines for non-CII OT.[21]

4. **Adopting technologies for cyber resilience through Public-Private Partnerships:** To address the deficit in OT cybersecurity solutions, the Masterplan aims to drive the further development of innovative solutions within Singapore's OT industry through the National Cybersecurity Research and Development Programme[22] and establish Security Operations Centres (SOCs) at the sectoral level to oversee, monitor, and coordinate cybersecurity efforts between Government agencies and CII owners.

Informing guidelines for OT: US guide to industrial control systems security

Published by the US National Institute of Standards and Technology (NIST), the guide helps enterprises involved with OT secure their ICS systems.[23] NIST developed the guide in partnership with public and private ICS enterprises, compiling several recommended measures to help OT enterprises meet their cybersecurity objectives. It provides both a set of substantive best practices for a government interested in OT cybersecurity and an example of a strong multi-stakeholder process through which to develop these. The NIST guide recommends that organizations and enterprises involved with OT:

- Segregate networks and devices
- Deploy security patches and mitigations quickly
- Restrict the ability to modify data
- Establish quick detection capabilities
- Ensure redundancy in systems
- Create an incident response plan to respond to incidents quickly
- Deploy a "defence-in-depth" strategy where cybersecurity mechanisms are layered to minimize the impact if a mechanism fails.

20 CSA, 1 October 2019, "Singapore's Operational Technology Masterplan". Available at: https://www.csa.gov.sg/-/media/csa/documents/publications/ot_masterplan/csa_ot_masterplan.pdf

21 CSA, "Cybersecurity Code of Practice for CII". Available at: https://www.csa.gov.sg/legislation/codes-of-practice. The CCoP prescribes measures that owners of CII systems are required to implement, and mainly covers IT systems to date.

22 National Research Foundation, "National Cybersecurity R&D Programme". Available at: https://www.nrf.gov.sg/programmes/nationalcybersecurity-r-d-programme

23 National Institute of Standards and Technology, May 2015, "Guide to Industrial Control Systems (ICS) Security". Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

In addition, NIST's Special Publication 800-53 (NIST SP 800-53) provides a catalogue of cybersecurity and privacy controls for federal information systems and organizations.[24] Organizations use NIST SP 800-53 to assess and select the relevant controls to help manage information security and privacy risks for government systems, which could be useful for other regimes seeking standards to draw on for things like procurement of OT. The controls in NIST SP 800-53 also help organizations comply with cybersecurity obligations under relevant security legislation, policies, and directives.

OT certification: EU cybersecurity act 2019

The EU has so far approached OT cybersecurity by focusing on a cybersecurity certification framework for ICT products that specifically includes OT, along with other services and processes through its Cybersecurity Act.[25] Certification frameworks represent an established best practice for governments and the EU example suggests how these can be usefully applied for OT. The EU certification helps enterprises and organizations that manage OT understand their risks and take necessary steps to ensure cybersecurity.

- The scheme certifies that OT – products, processes, and services – of EU companies have met one of three cybersecurity assurance levels (basic, substantial, or high) for their respective categories.[26]
- The certification scheme is voluntary. The EU also provides grants and subsidies to encourage enterprises to migrate from legacy or vulnerable OT systems to certified, secure OT systems, thus helping to spur innovation for OT cybersecurity.
- Two expert groups are established under the Act to help develop and implement the certification scheme:
  - The European Cybersecurity Certification Group (ECCG)[27] is comprised of representatives from Member States.
  - The Stakeholder Cybersecurity Certification Group (SCCG)[28] will be comprised of private entities, trade associations and academic institutions.

24 National Institute of Standards and Technology, "Special Publication 800-53". Available at: https://nvd.nist.gov/800-53

25 Regulation 2019/881 of the EU Parliament and Council, 17 April 2019. Available at: http://eur-lex.europa.eu/eli/reg/2019/881/oj

26 The European Commission, "The EU cybersecurity certification framework". Available at: https://ec.europa.eu/digital-singlemarket/en/eu-cybersecurity-certification-framework

27 The European Commission, "The European Cybersecurity Certification Group". Available at: https://ec.europa.eu/digital-singlemarket/en/european-cybersecurity-certification-group

28 The European Commission, "Call for applications for the selection of members of the Stakeholder Cybersecurity Certification Group". Available at: https://ec.europa.eu/digital-single-market/en/news/call-applications-selection-members-stakeholder-cybersecuritycertification-group

OT guidance from the private sector

The Operational Technology Cyber Security Alliance (OTCSA) is a coalition of OT industry organizations established to share cybersecurity resources, best practices, and guidelines with OT operators and suppliers that could prove useful to assist governments in the area of guidelines for CII and non-CII operators.[29] For example, OTCSA published a white paper in October 2019 on "Vulnerability Management for Operational Technology" that highlights known vulnerabilities in OT and recommends OT operators manage such vulnerabilities by (i) keeping an inventory of OT assets; (ii) building smaller, isolated and trusted networks to separate components, and (iii) developing and defining policy to identify assets and their respective threats, who should be responsible, and the mitigation strategy.[30]

ISACA is a global non-profit organization that that shares knowledge and standards among cybersecurity and IT professionals.[31] It published a 2016 whitepaper, "The Merging of Cybersecurity and Operational Technology," jointly with the International Society of Automation (ISA) to explore the securing of industrial systems/industrial Internet in a converging IT/OT environment.[32] The report includes a taxonomy of differences and similarities between OT and IT that might be useful to governments and recommends that enterprises should converge people working in IT and OT to match the convergence in systems which may be useful to governments in the area of training and capacity building. ISACA recommends OT operators cross-train IT and OT teams, harmonize their respective operations, and/or merge them into single business units. This allows the teams to understand each other's systems and cooperate to leverage common standards, risk, and governance approaches for OT.

Also in the area of guidelines for CII and non-CII operators, governments may consider a report published by Cisco Systems, "The Evolution of Industrial Cybersecurity and Cyber Risk White Paper", to help OT enterprises embrace digital transformation through a risk management lifecycle approach.[33] The report recommends that organizations adopt a cyber risk blueprint that designs their cybersecurity by considering best practices, regulations, the industry's specific use cases, expected threats and methods of mitigation, the use of leading cybersecurity products and services, automation of continuous cyber risk assessments, and purchasing cyber insurance to transfer cyber risks to a third party.

29 Operational Technology Cyber Security Alliance. Available at: https://otcsalliance.org

30 Operational Technology Cyber Security Alliance, "Vulnerability Management for Operational Technology". Available at: https://otcsalliance.org/wp-content/uploads/2019/10/Vulnerability_Management.pdf

31 ISACA. Available at: https://www.isaca.org

32 ISACA, "The Merging of Security and Operational Technology". Available at: https://www.isaca.org/bookstore/bookstore-wht_papersdigital/whpsot

33 CISCO, "The Evolution of Industrial Cybersecurity and Cyber Risk White Paper". Available at: https://www.cisco.com/c/en/us/solutions/collateral/industry-solutions/whitepaper-c11-742528.html

As it relates to OT standards, ISA/IEC 62443 represents a series of cybersecurity standards and technical reports for all industries and critical infrastructures to secure their industrial automation and control systems.[34] It was developed by the International Society of Automation (ISA) and adopted by the International Electrotechnical Commission (IEC). The ISA/IEC 62443 standard helps stakeholders address and mitigate cybersecurity vulnerabilities and ISA-62443-4-2 provides the technical requirements for cybersecurity components in ICS.[35]

Additionally on standards, the North American Electric Reliability Corporation's Critical Infrastructure Protection standards (NERC-CIP) specifies the minimum mandatory cybersecurity requirements for bulk power systems in the US, Canada, and Mexico. NERC-CIP helps stakeholders identify assets, implement cybersecurity and recovery plans, implement employee education sessions, and is enforced through audits, investigations, spot-checks, and self-reporting and certification.[36] Public consultations and ballots are held to review and amend the standards.[37]

Whether from the private or public spheres, a range of approaches can help inform governments in establishing a cybersecurity policy framework for OT. Once set, such a framework must be implemented.

34 ISA/IEC 62443. Available at: https://www.isa.org/store/products/product-detail/?productId=116731

35 ISA/IEC 62443-4-2. Available at: https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifiessecurity-capabilities-for-c

36 NERC-CIP. Available at https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

37 NERC, "Project 2016-02 Modifications to CIP Standards". Available at: https://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx

#3 Implementation

Steps to carry out the policy over time

- Create OT cybersecurity risk assessment mechanisms for appropriate CII and OT systems with guidelines that are continually updated and reviewed
- Encourage non-CII OT operators to adopt cybersecurity guidelines voluntarily
- Use the public sector to lead by example
- Collaborate with other countries to share cybersecurity knowledge and threat intelligence

Once a national strategy and policy for OT is in place, governments must implement and track the policy to ensure its operationalization.

To help broaden the uptake of OT cybersecurity requirements, a country's OT cybersecurity regime should include risk assessments (which can be self-conducted or conducted by a government agency) to evaluate on a regular basis if a designated CII has adequate cybersecurity measures in place. The risk assessments should also be available for non-CII enterprises to evaluate their cybersecurity measures and identify any shortcomings.

In this regard, non-CII enterprises may adopt the same OT as CII enterprises. Though the cybersecurity guidelines focused on CII operators, governments should encourage non-CIIs to adopt the guidelines to create a more robust cybersecurity regime in the country.

Governments can be important leaders in encouraging uptake. For example, implementation of guidance in public agencies or publicly owned infrastructure can be an important demonstration to the market. Rules conditioning government procurement or contracting on policy implementation can also facilitate quicker uptake and incentivize organizations to implement better OT security.

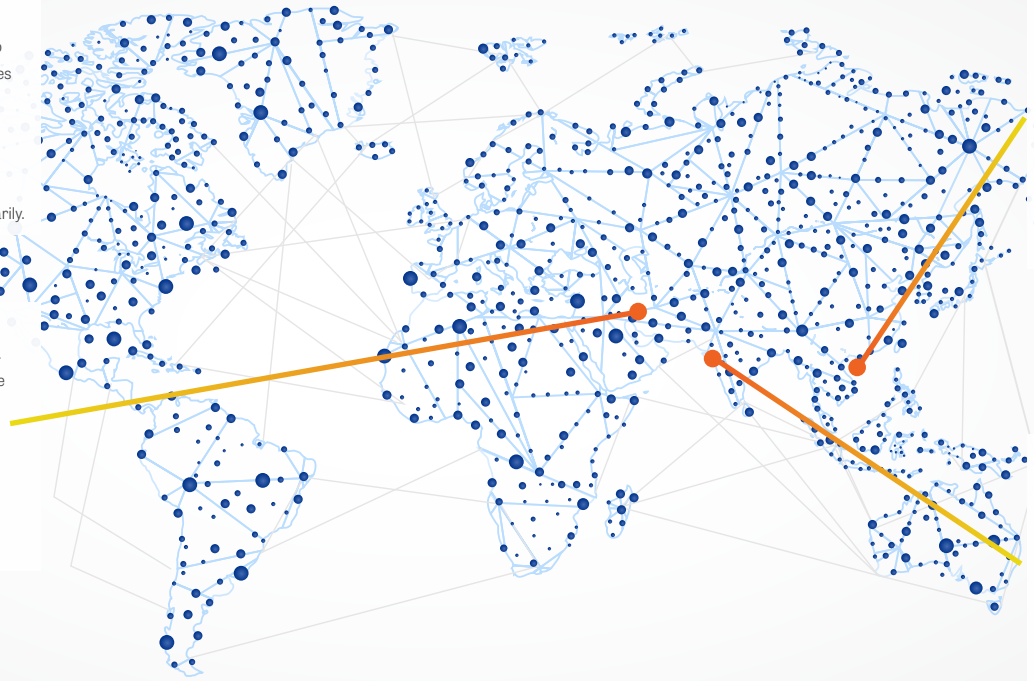
Also, governments can help establish networks to share information not just within a country, but across borders as well. Whether this be done through developing networks of OT-ISACs, led by sector-level agencies, or through global private networks like the Operational Technology Cyber Security Alliance (OTCSA) and ISACA, as discussed above, joining global information-sharing networks to coordinate on real-time threats offers a range of benefits to participating countries and industry partners. Industry involvement in these networks is key to ensuring their success and industry can participate or lead in training, share expertise, best practices, and skills across cybersecurity professionals in both companies and governments.

SNAKE infiltrates global auto manufacturing: Honda shuts factories around the world due to the SNAKE ransomware in June 2020. Written specifically to attack Honda, the ransomware had spread through its internal network to several of its factories around the world, disrupting operations at the factories for about 3 days. Honda did not reveal how the ransomeware entered its networks, but speculation was that the breach was due to telework policies from COVID-19.

How could government policy have helped?
Encouraging non-CII OT operators to adopt cybersecurity guidelines voluntarily.

Bahrain's electricity and water systems shut down: Several systems of Bahrain's Electricity and Water Authority were shut down by hackers in 2019. The hackers were suspected to be state-sponsored actors from Iran, and the cyberattack occured amidst growing tensions between Bahrain and Iran. This attack was believed to be a test run of Iran's capability to disrupt the country.

How could government policy have helped?
Establishing OT training and capacity building for organizations and employees.



WannaCry hits fab: In 2018, more than 10,000 computers and fabrication tools in Taiwan Semiconductor Manufacturing Company's (TSMC) fabrication plant were infected with a WannaCry variant, causing a 24-hour production halt and a recovery process which took several days. The attack resulted in a financial performance drop of 2%, about USD 170 million.

How could government policy have helped?
Establishing a cybersecurity network among sector-level oversight organizations, CIIs, and OT enterprises to establish a two-way reporting system, coordinate efforts for rapid incident response, and share cybersecurity knowledge and threat intelligence.

Petya halts port traffic: India's largest container port, JNPT, was hit by Petya ransomware in 2017. Operations at the Gateway Terminals India in JNPT port were stalled as the Petya ransomware attack brought down its systems, leading to a clogging of cargo. The operator of the terminal, Maersk, lost about USD 300 million in revenue globally as the infection was spread in its global network.

How could government policy have helped?
Developing and publishing OT cybersecurity guidelines for CII and non-CII operators, drawing from best practices and relevant international standards.

Figure 3: Cyberattacks on OT in Asia and how policy could have helped[38]

Conclusion

The convergence of OT with IT has opened a whole new range of innovation and opportunities for businesses, organizations, and societies to leverage OT systems in ways unimaginable only a few years ago. At the same time, this convergence has drastically increased the cybersecurity threat environment for OT. Governments in Asia and globally are continually upgrading their cybersecurity policies to address evolving threats and protecting OT is rapidly rising as a priority for many regulators tasked with protecting their countries' critical infrastructure, national economic interests, and safety of citizens.

The cyber threat to OT is real. Figure 3 above highlights some cases of cyberattacks on OT in Asia and their impact, along with a recommendation from the checklist on how the attack may have helped mitigate or reduce the impact of the attack.

Governments seeking to establish or upgrade their cybersecurity policies to better account for OT can leverage the checklist in this report as a useful point of departure. The checklist seeks to help authorities identify which elements may already be in place, which are not, and to serve as a general guide to how authorities and OT operators can work together to improve cybersecurity for OT. A reference guide to support governments further can be found in Appendix A.

Cybersecurity for OT and the relevant policy structures to support these are continually shifting. As such, decisions and actions considered and undertaken by governments should be reviewed again in the future to account for the shifting threats to OT. Over time, the current separation between OT and IT will likely fade as systems fully converge. As governments successfully build out their cybersecurity policy architecture for OT, in the long-run, OT will simply become one among many elements of a mature cybersecurity policy regime.

Published by: Access Partnership

38 (previous page)

Skybox, 8 October 2018, "TSMC WannaCry Hits OT Plants with a Hefty Price Tag". Available at: https://blog.skyboxsecurity.com/tsmcwannacry;

The Economic Times, 28 June 2017, "Petya ransomware: Government working with Maersk to resolve situation at JNPT". Available at: https://economictimes.indiatimes.com/tech/internet/petya-ransomware-government-working-with-maersk-to-resolvesituation-at-jnpt/articleshow/59357881.cms;

Ben Dooley and Hisako Ueno, 12 June 2020, "Honda Hackers May Have Used Tools Favored by Countries". Available at: https://www.nytimes.com/2020/06/12/business/ransomware-honda-hacking-factories.html;

Bradley Hope, Warren Strobel and Dustin Volz, The Wall Street Journal, 7 August 2019, "High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran". Available at: https://www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488

Appendix A

OT Policy Resources

If you are interested in more information regarding OT cybersecurity, below is a list of additional resources on OT across Asia and globally.

Entity	Name of resource	Source
Institutional foundation		
Japan	Basic Act on Cybersecurity (English)	http://www.japaneselawtranslation.go.jp/law/detail/?ft=5&re=02&dn=1&gn=4&sy=&ht=A&no=104&x=0&y=0&ia=03&ja=04&ky=&page=3
Singapore	Cybersecurity Act	https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312
Organization for Economic Co-operation and Development (OECD)	Recommendation of the Council on the Protection of Critical Information Infrastructures	http://www.oecd.org/sti/40825404.pdf
National strategies		
Cyber Security Agency of Singapore (CSA)	Singapore's Operational Technology Masterplan	https://www.csa.gov.sg/-/media/csa/documents/publications/ot_masterplan/csa_ot_masterplan.pdf
European Commission	Europe's moment: Repair and prepare for the next generation	https://ec.europa.eu/commission/presscorner/detail/en/ip_20_940
Australia's Department of Home Affairs	Australia's Cyber Security Strategy 2020	https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy
Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC)	The Cybersecurity Policy for Critical Infrastructure Protection	https://www.nisc.go.jp/eng/#sec4

Entity	Name of resource	Source
National codes and guidelines		
Cyber Security Agency of Singapore (CSA)	Cybersecurity Code of Practice for CII	https://www.csa.gov.sg/legislation/codes-of-practice
European Commission	Cybersecurity Act (for EU's certification framework)	https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework
US National Institute of Standards and Technology (NIST)	Guide to Industrial Control Systems Security	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
Australian Cyber Security Centre	Information Security Manual	https://www.cyber.gov.au/acsc/view-all-content/ism
US National Security Agency	Seven Steps to Effectively Defend Industrial Control Systems	https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/seven-steps-to-effectively-defend-ics.cfm
Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC)	Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure	https://www.nisc.go.jp/eng/pdf/principles_ci_eng_v5.pdf
Private sector guidance on OT		
Operational Technology Cyber Security Alliance (OTCSA)	Vulnerability Management for Operational Technology	https://otcsalliance.org/wp-content/uploads/2019/10/Vulnerability_Management.pdf
ISACA	The Merging of Cybersecurity and Operational Technology	https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsot
Cisco Systems	The Evolution of Industrial Cybersecurity and Cyber Risk White Paper	https://www.cisco.com/c/en/us/solutions/collateral/industry-solutions/whitepaper-c11-742528.html
International Society of Automation (ISA)	ISA/IEC 62443	https://www.isa.org/products/isa-62443-1-1-2007-security-for-industrial-automat
North American Electric Reliability Corporation (NERC)	Critical Infrastructure Protection (CIP) standards	hhttps://www.nerc.com/pa/Stand/Pages/CIP-Standards.aspx
Risk assessment mechanisms		
Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC)	Risk Assessment Guide Based on the Concept of Mission Assurance in Critical Infrastructure	https://www.nisc.go.jp/eng/#sec4
US National Institute of Standards and Technology (NIST)	Guide to Industrial Control Systems Security	https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
Cyber Security Agency of Singapore (CSA)	Guide to Conducting Cybersecurity Risk Assessment for CII	https://www.csa.gov.sg/legislation/supplementary-references

With special thanks to the
Cyber Security Agency
of Singapore

CSA SINGAPORE

COALITION FOR CYBERSECURITY IN ASIA-PACIFIC

The Coalition for Cybersecurity in Asia-Pacific comprises Amazon Web Services, Becton Dickinson, Cisco Systems and VMware.

Access Partnership

+65 9145-6137
singapore@accesspartnership.com
www.accesspartnership.com