Deloitte.

Building cyber security into critical infrastructure

Protecting industrial control systems in Asia Pacific

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Foreword

The critical infrastructure that provides energy, water supply, transportation, and telecommunication—the foundations of our societies and economies—is fundamentally changing due to the digital revolution. Mission-critical assets and processes enabling these essential industries are powered by operational technology (OT) with industrial control systems (ICS) making up the key components. Unfortunately, infrastructure operators are not always equipped to protect these environments against modern cyber security threats, which have become amplified since COVID-19.

In fact, the attack surface and risks to both OT and information technology (IT) are increasing significantly. This is due to the ongoing convergence of IT and OT, and the emergence of Industry 4.0 ecosystems relying on highly connected devices, including the industrial internet of things (IIoT). At the same time, the increasing sophistication of today's threats leaves our legacy OT and ICS—prevalent in critical infrastructure sectors—more vulnerable to attack than ever before, as seen with various incidents over the past decade in Asia Pacific and beyond. The resilience of our essential infrastructure to cyber attacks needs vast and overdue improvement. Yet we find ourselves at a critical juncture as the challenge of securing these infrastructures grows with the blurring of boundaries between IT and OT, and disruptive technological innovations that introduce further complexity.

The Asia Pacific region is diverse, from society and economies to infrastructure and technology, and this diversity is reflected in the region's critical infrastructures. This paper examines the changing risk landscape in Asia Pacific, which is evolving with the rapid pace of economic growth and technology leadership. These are hallmarks of a highly dynamic region gripped by unrelenting competition and ever-present geopolitical tensions. We then highlight key challenges facing Asia Pacific critical infrastructure operators looking to protect their mission-critical assets and processes against cyber threats, before delving deeper into how these issues can be overcome and outlining the key steps to achieve this effectively and efficiently.

Drawing on our global and regional experience assisting critical infrastructure organisations to deal with cyber incidents and improve their cyber defences, and on consultations with our Asia Pacific leaders and specialists, this paper aims to help leaders—from executive teams and security leaders to engineering and operations—develop their strategies and plans for greater cyber resilience.

We hope that this view on building cyber security into critical infrastructure in Asia Pacific provides you with helpful insights as you work to further protect your most essential assets and services.

Sincerely,

Max Y. Lin
Asia Pacific Cyber OT/ICS & IoT leader
Deloitte

James Nunn-Price
Asia Pacific Cyber leader
Deloitte

Growing complexity, growing risk

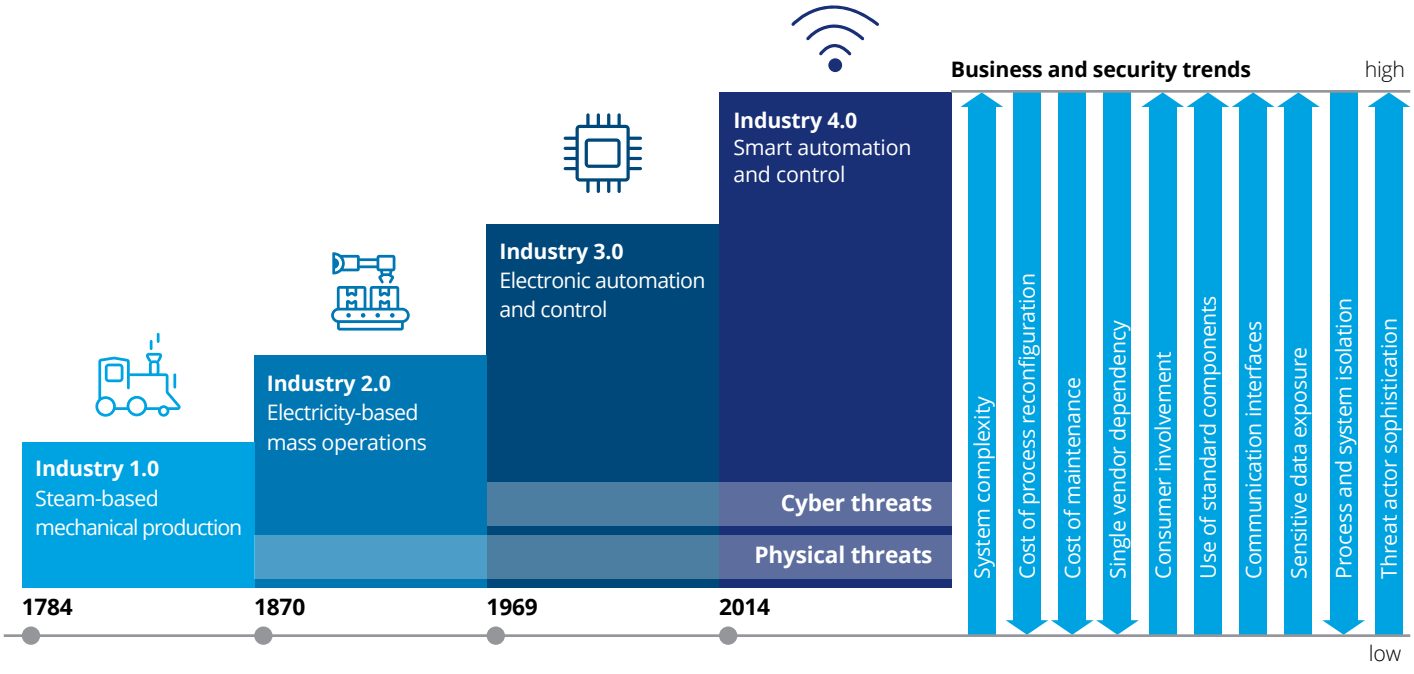
The increasingly complex infrastructure landscape

To a large extent, operational technology (OT) has historically operated independently from corporate information technology (IT) systems with business tasks and teams on one side, and industrial processing on the other. At the heart of OT, industrial control systems (ICS) were based on different standards designed by vendors using proprietary languages and protocols. ICS components were used in closed loops and could not communicate with devices from other vendors, let alone IT networks. Due to their physical isolation from other environments and their use of purpose-built technologies, operational infrastructure relying on ICS largely benefitted from a natural buffer—or "air gap"—from cyber threats.

Yet they were not completely immune: true air gaps only existed in rare maximum-security sites while plant computers, left unchecked and exposed through internet modems, could easily be compromised and leveraged to create chaos. Industrial systems became increasingly connected as they progressively adopted internet protocols and standards, eroding the natural buffer that shielded them. And that buffer can be bypassed: even when air gaps are implemented correctly, common operational scenarios require engineers to plug in external USB flash drives—the means through which Stuxnet is understood to have infected an Iranian uranium enrichment plant.[1]

Operational processes now involve more modern software, data, and networks, which require integration with IT systems. This convergence of IT and OT can be observed nearly everywhere as organisations—including those that provide energy, water, telecommunication, transport, and other essential services—further digitise their systems and processes to be more efficient and reliable. The buffer is disappearing (Figure 1).

Figure 1: Progression of cyber and physical threats for each industrial revolution



OT, ICS and related technologies

Industrial Internet of Things (IIoT)

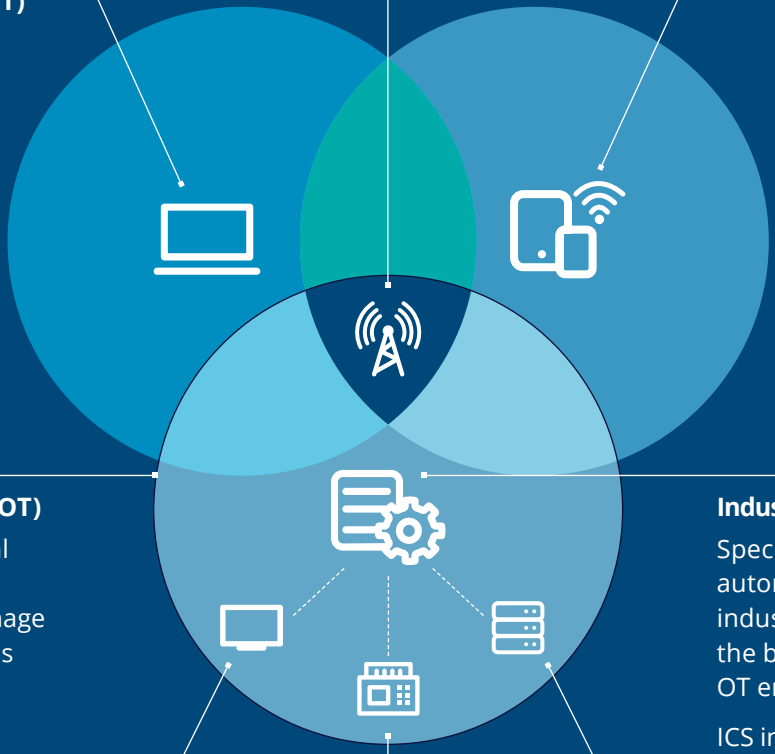
IoT technologies applied to industrial environments, such as temperature monitoring sensors sending data to analytics solutions in the cloud. These are increasingly found in operational sites leveraging Industry 4.0 concepts.

Information technology (IT)

Computers, devices and networks supporting business processes such as customer relationship management and production planning.

Internet of Things (IoT)

Connected objects and devices that communicate over networks to exchange data or take action, such as wearables and smart home devices.



Operational technology (OT)

The ecosystem of technical systems and devices that support, monitor and manage physical operations such as an oil refinery process.

This also includes IT-like systems such as computer workstations.

Industrial Control Systems (ICS)

Specialised systems that automate and control industrial processes. These are the bulk of what is found in an OT environment.

ICS include components such as DCS, SCADA and PLCs.

Supervisory Control and Data Acquisition (SCADA)

Event-driven ICS architecture particularly suited for monitoring and controlling geographically distributed operational sites.

Programmable Logic Controllers (PLCs)

Industrial devices that monitor and control a physical mechanism—such as a water pump—based on programmed parameters.

PLCs are key building blocks of ICS.

Distributed Control System (DCS)

Process-focused ICS architecture controlling operations at the site level.

Accelerating this trend, leaders are transitioning to Industry 4.0 to help propel their businesses forward. Industry 4.0, also known as the Fourth Industrial Revolution, "refers to the marriage of physical assets and advanced digital technologies—IoT, artificial intelligence (AI), robots, drones, autonomous vehicles, 3D printing, cloud computing, nanotechnology, and more—that communicate, analyze, and act upon information, enabling organizations, consumers, and society to be more flexible and responsive, and make more intelligent, data-driven decisions".[2]

Organisations are adopting Industry 4.0 use cases such as performance and predictive maintenance analytics, which typically rely on IIoT sensors feeding operational data to enterprise or cloud-based solutions. These technologies allow critical infrastructure operators to become more agile, improve their customer service, and better manage their assets 24 hours a day, 7 days a week. The COVID-19 pandemic has further increased these needs as many operators are required to maintain assets and services while isolating away from facilities.

These technologies greatly add to an organisation's digital data and connectivity requirements. OT and IT systems are becoming not only more integrated, but also larger and more complex to support these additional use cases. IIoT offers huge potential across many sectors, but it generally requires shuffling large amounts of data between OT assets (often in many locations) and cloud services. An ever-expanding interconnectivity underpins these additional communications.

As a result of this integration trend, organisations present an expanding attack surface for cyber threats and face greater risks to both their OT and IT systems. Avenues for cyber attacks against critical systems are on the rise as IT/OT boundaries become increasingly porous and network perimeters expand to the cloud. Even relatively basic threats like generic internet worms have been known to bring down corporate IT and production sites alike. In many cases, this is due to a lack of system patching and network segmentation, as was seen with a steel plant hit by the common Conficker malware years after a patch was issued.[3]

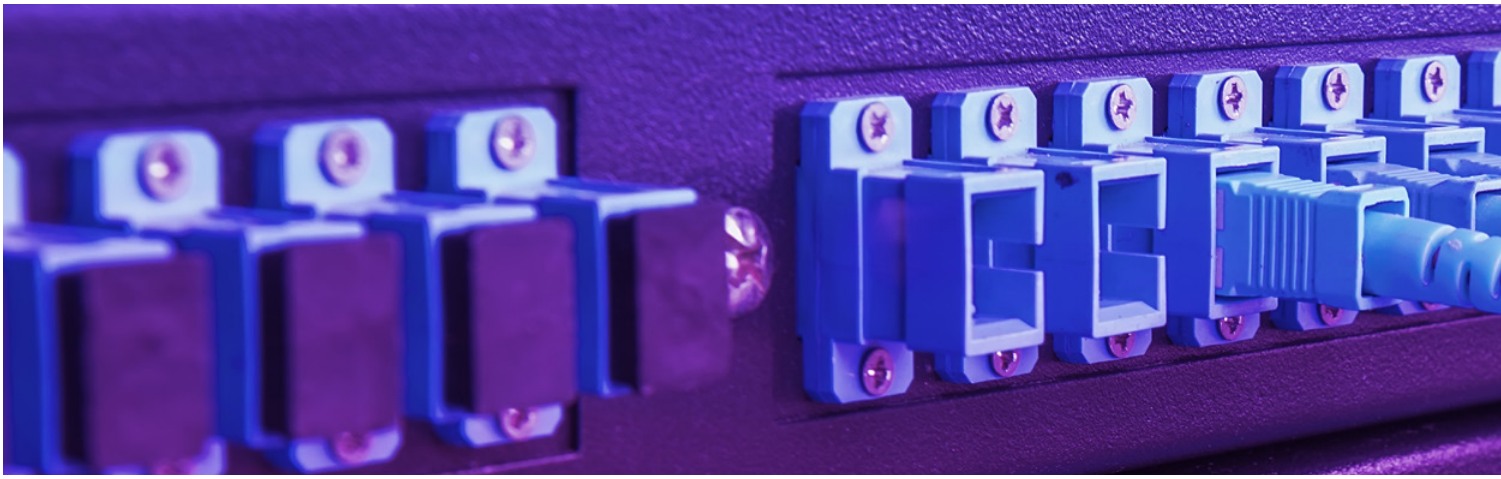
At the same time, more sophisticated threats such as some recent ransomware and state-sponsored attacks are becoming increasingly prevalent, as seen with NotPetya. NotPetya is thought to have inflicted more than US$10 billion in damages and interrupted global operations for the world's largest container shipping company at a cost upwards of US$250 million.[4]

Yet the impacts of cyber attacks can go beyond operational downtime and financial hardship. Consider a city-wide loss of power as in the 2015 attack on the Ukraine power grid at a sustained level, and its impact on essential services.[5] This is just one of countless scenarios where an attack on OT systems could have devastating consequences, such as shutting down hospitals treating patients in intensive care units. But these scenarios are not limited to domino effects, as OT failures can directly result in injuries or fatalities. In 2017, a widely reported attack on a Saudi Arabian petrochemical plant was designed to cause physical damage and could have injured workers.[6]

Avenues for cyber attacks against critical systems are on the rise as IT/OT boundaries become increasingly porous and network perimeters expand to the cloud.

The security and safety of critical infrastructure around the world are at risk, and that risk is mounting. For decades, Asia Pacific has been at the forefront of connectivity and this has only accelerated with rapid economic growth. The region is forecast to lead the world in IoT deployments by a wide margin, including an expected 65% of global 5G subscriptions by 2024.[7]

As these developments lead to exponential exposure of both consumer and industry systems, it is essential to look at how we can tackle existing and looming security challenges. Fortunately, in addition to leading in IoT deployments, Asia Pacific also seems set for the highest growth in cyber security spending on critical infrastructure. A study by ABI Research anticipates a compound annual growth rate (CAGR) of almost 12% over a 7-year period to 2025.[8] Globally, the OT segment is also forecast to grow at the fastest rate.[9] Despite these encouraging predictions, more focus is needed to tackle serious risks growing at an even higher speed.



Ensuring the security of our infrastructure

The good news is that several standards and frameworks have been defined to help critical infrastructure operators improve the security posture of their ICS and form a resilient foundation for an OT cyber security program.

Notable cyber security standards

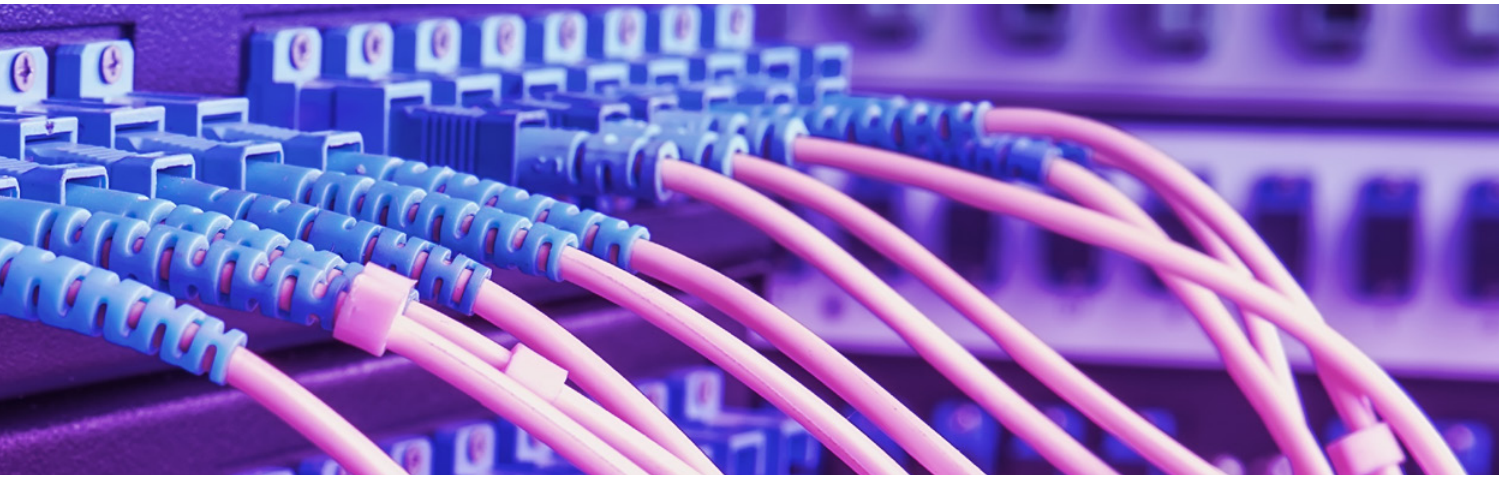
- ISA/IEC 62443: A series of standards, developed by an International Society of Automation (ISA) committee and adopted by the International Electrotechnical Commission (IEC), that are designed to address ICS security vulnerabilities.[10]
- The National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF): The US agency's cyber security framework for critical infrastructure, comprising five pillars of risk management practices,[11] supported by technical guidance on ICS security controls provided in special publication SP800-82.[12]
- The North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP): A set of mandatory cyber security standards focused on critical assets at North American organisations participating in the US electrical grid.[13]
- The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2): The US Department of Energy's maturity model and implementation guidance for cyber security in the power sector.[14]

Regulators and critical infrastructure operators around the world are adopting these references to help address long-standing cyber risks. Increasing use of internationally recognised standards is being seen in the Asia Pacific region from China to New Zealand, with the latter building on NERC CIP and the NIST CSF to develop its guidelines. Another example is Australia, which is leveraging sector-specific frameworks such as the ES-C2M2 for its power grid cyber resilience initiative (see Appendix: Highlights of resilience efforts in Asia Pacific).

However, it is evident that governments, organisations, and even standards are playing catch-up with the evolving cyber threats to critical infrastructure. While these threats evolved over decades, OT systems were seldom overhauled and the majority still lack built-in security features. Such legacy infrastructure (the "brown field") presents a double challenge: systems are particularly vulnerable and also difficult to protect as this requires retrofitting security controls to environments not designed with security in mind. This is particularly true for essential services, as stability was prioritised over modernity to maximise reliability and protect the safety of workers and the public. Critical infrastructure operators are now being forced to act as they recognise these goals are at risk.

To address this challenge, a recent breed of cyber security solutions has been developed with inherent understanding of how even legacy OT systems communicate, function, and operate. These specialised solutions can help organisations map out their current ICS asset landscapes, and their ongoing threats and vulnerabilities. In turn, newer ICS architectures and components are now increasingly being built with "security by design" at the forefront by leveraging OT security guidelines, standards, and blueprints.

In the next sections, we delve deeper into the landscape of critical infrastructure cyber threats and challenges in Asia Pacific, what is needed to effectively address them, and how organisations can best embark on the path towards greater cyber resilience.



Threats and challenges facing critical infrastructure operators in Asia Pacific

Critical infrastructure operators in Asia Pacific face a diverse range of ever-increasing cyber threats, a reflection of both established and evolving geopolitical tensions and competition in a sometimes volatile region ripe with power imbalances. These threats range from non-targeted, yet potentially devastating, ransomware to sophisticated attacks engineered by nation states and associated threat actors supporting their agendas. Proper situational awareness is essential to focus on the threats that put safety and security most at risk. This does not come without organisational and technical challenges, such as a general lack of visibility into operational systems and processes, which need to be understood early to avoid pitfalls on the path to resilience. Here we explore some of the common threats and challenges to consider from the outset.

Threat actors

Nation states and cyber warfare groups

State-funded groups present a major threat to critical infrastructure, as they can use sophisticated methods and have access to advanced intelligence and tools to break into organisations' OT systems and compromise the operation of their assets.

These threat actors may compromise another nation's information network and supply grids to cause maximum disruption to critical services such as water, gas, and electricity. This is increasingly being used by some nation states as a way to increase economic, political, or diplomatic pressure on the other nation. In this context, it is worrying that one of the most potent cyber warfare groups is now turning its attention to Asia Pacific power grids.[15]

Insiders and third parties

Individuals within critical infrastructure operators, such as present or past employees, third-party contractors, and supply chain partners—even tax software suppliers as seen in the NotPetya attack[16]—can pose a significant risk. For example, a rogue employee could potentially insert malicious code into smart meters to disrupt and cause damage to a power grid.[17] With access to sensitive business or operational systems and blueprints, individuals and vendors alike can either intentionally or unintentionally compromise critical infrastructure organisations from within.

These threats often take advantage of gaps in monitoring systems and the lack of effective third-party risk management (TPRM) processes.

Hacktivists

"Borderless" groups can hack into systems operating critical infrastructure or sabotage critical services through activities such as Distributed Denial of Service (DDoS) attacks.

Figure 2 (on the next page) outlines several recent examples of cyber attacks on critical infrastructure in the Asia Pacific region.

Challenges

Awareness

Many critical infrastructure operators are hampered by limited awareness that their OT systems are vulnerable to cyber security risks. Without a sound understanding of the threat, they are likely to struggle to develop effective mitigation strategies in advance of an incident occuring.

Visibility

Few critical infrastructure operators have full or even partial visibility of their OT assets, seeing them as a "black box". As a result, they often have little insight into how their OT assets are configured or operate on a day-to-day basis.

Building an accurate inventory of OT assets is one of the biggest challenges facing critical infrastructure operators, but it is essential for evaluating and protecting against cyber risk.

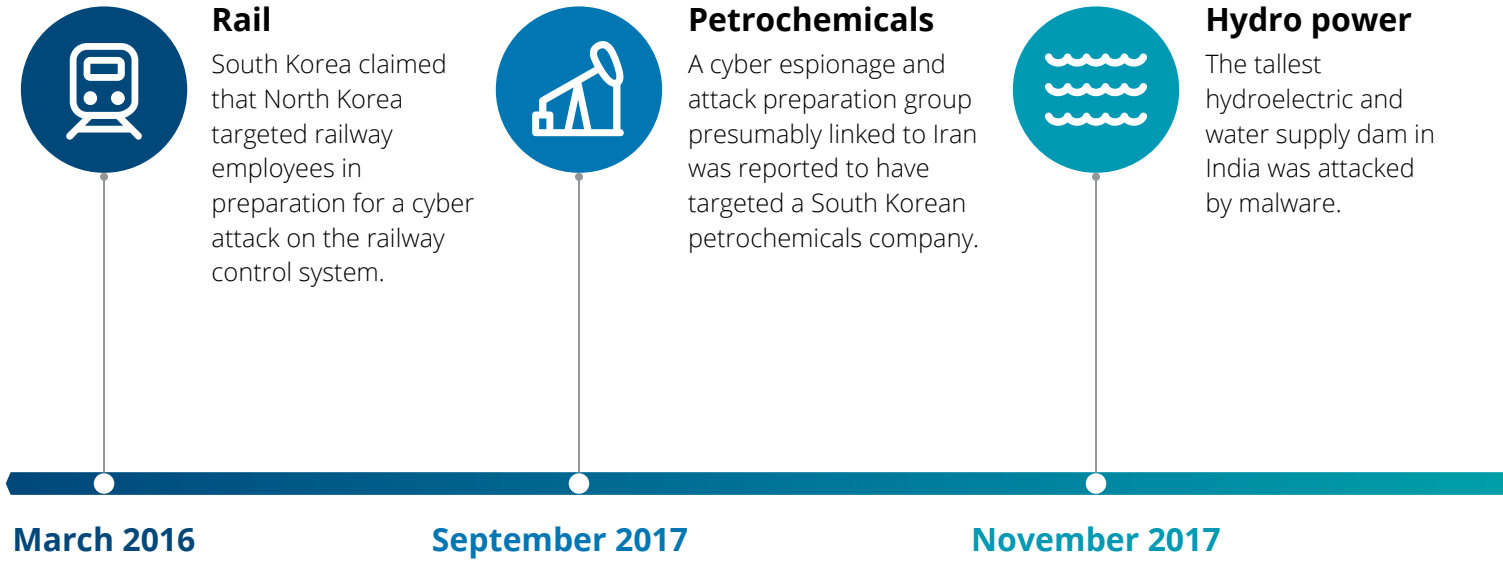
In addition, many organisations lack effective monitoring solutions and processes. This can result in an incomplete view into the OT assets and reduced situational awareness, both of which can make organisations more vulnerable.

Maintenance

SCADA and legacy ICS and components often cannot be updated or have security patches applied. Even if they exist, such updates would be limited to maintenance windows for wider infrastructure upgrades, which in some cases may not occur for long periods of several years or more. As safety and reliability are the top concerns for operators, and OT environments were believed largely immune to cyber threats, organisations have unsurprisingly given stability a much higher priority than cyber security.

Yet even with more aggressive security patching and maintenance strategies, these OT systems cannot generally match the patching capabilities of IT environments, increasing the need for virtual patching, up-to-date and deep visibility of vulnerabilities, and threat hunting and detection.

Figure 2: Critical infrastructure cyber attacks in Asia Pacific



Source: Deloitte analysis; news reports.[18]

Challenges (continued)

Segmentation

A long-established method of protecting sensitive systems is to segment networks into security zones guarded by firewalls and other access control techniques. This was not the case a few decades ago, when "flat" networks were designed without security in mind.

Today's industrial networks still often lack these basic controls, for several reasons. First, OT network infrastructure is typically left untouched unless facilities undergo major overhauls. Second, as firewalls were designed for IT environments rather than OT, they were not well-suited to integration with industrial networks and protocols. Finally, the visibility problem means that cyber security teams usually lack an understanding of normal, or baseline, network traffic. Without a reliable map of OT assets and their network communications, industrial engineers understandably cannot allow firewalls to be deployed in their environments due to the strong possibility of operational disruption.

Incident response

The majority of critical infrastructure organisations have no (or very limited) incident response plans for their OT systems, nor do they have playbooks for their OT environments. Without strong processes in place, they cannot enact comprehensive and effective responses to cyber threats.

Governance

These challenges, particularly the lack of incident response plans, highlight the need to develop a comprehensive OT security governance strategy that bridges gaps—including the often significant culture differences—between IT and OT teams. However, this is not easy and requires overcoming significant challenges, such as gaining full visibility of OT assets and processes, and assigning cyber security roles and responsibilities for these assets and their interfaces with corporate systems and IT infrastructure.

Electric utilities

The dangerous cyber sabotage group behind the potentially destructive Trisis/Triton attack was revealed to be targeting electric utilities in Asia Pacific.

February 2019

Nuclear power

The IT network of the largest nuclear power plant in India was compromised by a cyber espionage group thought to act for North Korea.

September 2019

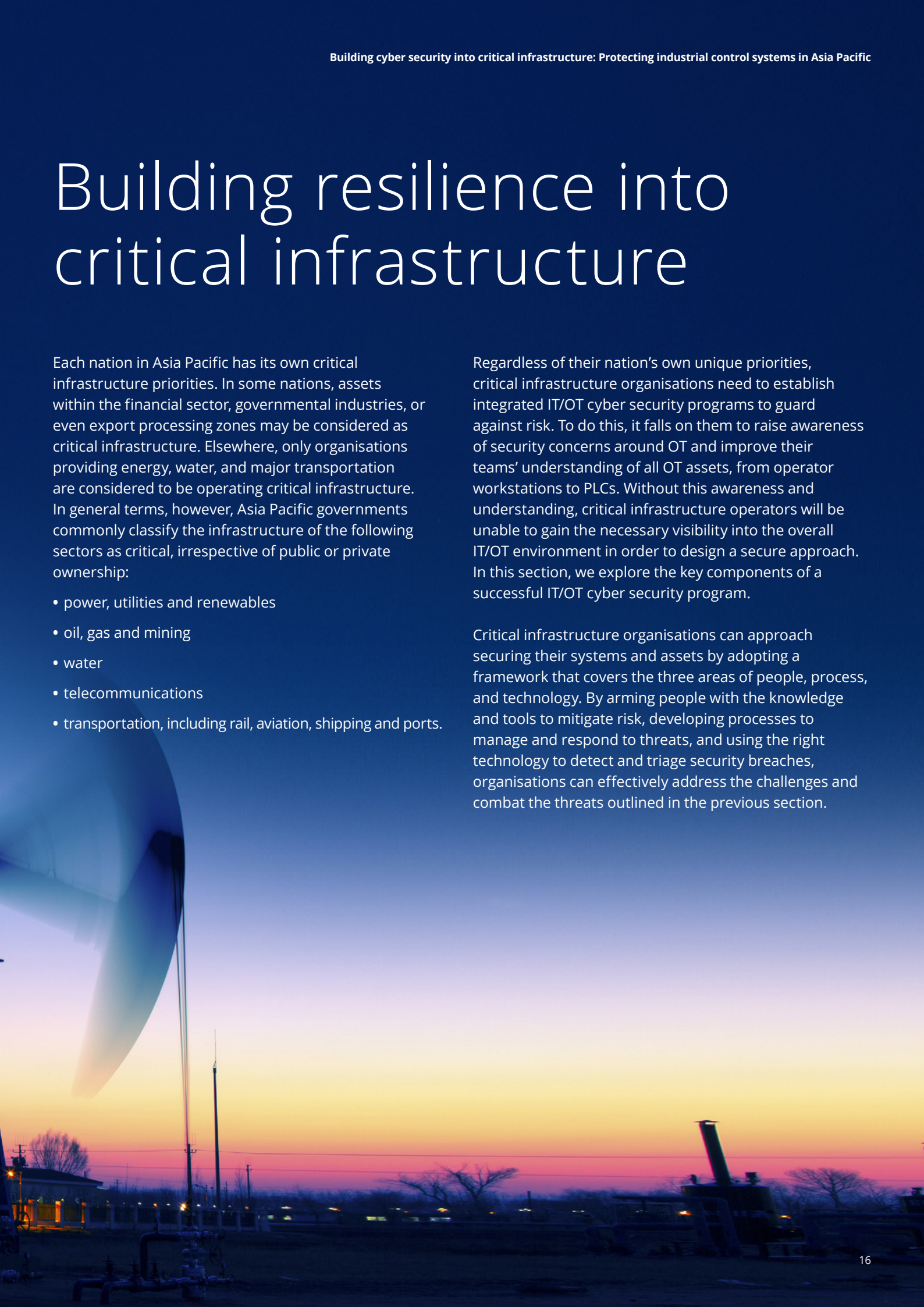
Building resilience into critical infrastructure

Each nation in Asia Pacific has its own critical infrastructure priorities. In some nations, assets within the financial sector, governmental industries, or even export processing zones may be considered as critical infrastructure. Elsewhere, only organisations providing energy, water, and major transportation are considered to be operating critical infrastructure. In general terms, however, Asia Pacific governments commonly classify the infrastructure of the following sectors as critical, irrespective of public or private ownership:

- power, utilities and renewables
- oil, gas and mining
- water
- telecommunications
- transportation, including rail, aviation, shipping and ports.

Regardless of their nation's own unique priorities, critical infrastructure organisations need to establish integrated IT/OT cyber security programs to guard against risk. To do this, it falls on them to raise awareness of security concerns around OT and improve their teams' understanding of all OT assets, from operator workstations to PLCs. Without this awareness and understanding, critical infrastructure operators will be unable to gain the necessary visibility into the overall IT/OT environment in order to design a secure approach. In this section, we explore the key components of a successful IT/OT cyber security program.

Critical infrastructure organisations can approach securing their systems and assets by adopting a framework that covers the three areas of people, process, and technology. By arming people with the knowledge and tools to mitigate risk, developing processes to manage and respond to threats, and using the right technology to detect and triage security breaches, organisations can effectively address the challenges and combat the threats outlined in the previous section.



People

Effective people management is the first step in building a resilient cyber security program. Without clearly defined roles, organisations will find it extremely difficult to achieve their OT cyber security objectives and may spend more time and resources than necessary. It is also essential to address the governance challenge outlined in the previous section.

It is important to not just define individual roles and responsibilities, but to align these roles to organisational security objectives. Personnel management may involve organising new security processes and changing staffing practices, but it can also involve other complexities.

To build a secure front against cyber risks, organisations need to:

- educate everyone in the organisation, from the board to field operators, on OT cyber risks to help prepare for change
- define roles and responsibilities that are specific to OT cyber security
- establish an OT cyber security training process for employees in these roles
- design robust industrial cyber security and cyber defence services, and familiarise employees with these services
- develop OT cyber security working groups, while establishing clearly defined communication channels between team members.

Working groups need to be cross-functional to bridge the gap between IT and OT security. But how do you get people with different skills, cultures, and priorities to collaborate effectively on responding to cyber incidents that involve both IT and OT assets, or that require IT security support to resolve OT incidents? Temporary transfers between the IT and OT teams can help build awareness and relationships, and defining roles and responsibilities in cross-functional teams is essential to ensuring clarity.

Process

From policies to procedures, the development of strong underlying processes is a vital step for critical infrastructure organisations if they are to build cyber security and resilience into their OT environments. Without defined processes, team members will find it difficult to effectively manage risks and secure operations.

To design processes that will protect OT systems from cyber threats, organisations need to:

- define the current state of their OT cyber security environments
- outline the target state of these environments and formulate long-term plans to achieve it, while ensuring team members are in alignment over the target
- identify and agree on good practices for achieving the target
- define manageable metrics to measure risk reduction and other achievements, and clearly outline short-term, medium-term, and long-term goals
- gain stakeholder approval while designing a resilient, effective OT cyber security program that will enable the organisation to achieve the target state
- use tools such as tabletop exercises and gamification (simulating certain scenarios) to develop incident response plans and playbooks that will help test procedures
- define supply-chain procedures and outline standards for third-party vendors to manage cyber security risks
- develop continuous risk management processes including monitoring evolving risks, threats, and compliance requirements; identifying and even anticipating required changes; and iterating all security capabilities and processes. These are essential to ensure an organisation's transformation does not become a one-off exercise.

All these processes, together with the roles and responsibilities assigned to an organisation's people, should come together to form the OT cyber governance framework.

Electric utility – Horizon Power

The Western Australia power company is pioneering large-scale use of real-time control Distributed Energy Management Systems supported by smart meter technologies.

To address its increasing OT cyber risk exposure, the company leveraged the ES-C2M2 cyber maturity model and moved towards adopting the NIST Cyber Security Framework.

Jeff Campbell, Chief Information Security Officer (CISO) at Horizon Power, also focused heavily on bringing a cyber security culture to OT teams, starting with embedding OT engineers in the IT security team and bringing them to briefings at the Western Australian government's Joint Cyber Security Centre.

Technology

OT-aware cyber security technologies and specialised solutions are important tools for helping critical infrastructure organisations protect their assets and mitigate potential risks. The right technology can help by providing OT teams with more visibility into operations as an enabling first step to implement further controls.

These technical controls should not just focus on policing the perimeter of an organisation's OT environment. For an organisation to achieve operational resilience, the scope needs to be expanded to the entire internal OT landscape, with adequate controls in place to protect the most critical assets and systems. However, it is also essential that new technologies do not disrupt operations, even if it means introducing fully passive, rather than active, OT security controls—at least initially.

To develop a resilient technology architecture for risk management, organisations need to:

- define and detail their OT-related network architecture, applications, databases, communication conduits, and other relevant assets
- ensure they have adequate network security controls and segmentation
- deploy secure remote access technology for both in-house operators and third parties, with specific permissions for different roles
- deploy threat detection and hunting solutions to identify existing compromises and ongoing attacks
- consider, under the right conditions, ICS-aware deep packet inspection firewalls that can also be triggered by events detected by threat monitoring solutions
- roll out permission management tools to effectively control access to OT systems
- establish an effective security monitoring system, and in doing so, increase situational awareness by collecting and processing critical OT data
- perform regular backups and integrate this process with the incident response program
- deploy effective early warning systems, such as honeypots, to detect unauthorised attempts to access OT systems.

Securing critical infrastructure against cyber threats is not a one-person, one-team, or even one-company job.

People, process, and technology are the three major pillars for building secure critical infrastructure. Securing critical infrastructure against cyber threats is not a one-person, one-team, or even one-company job. As well as securing their own operations, critical infrastructure operators in Asia Pacific would do well to further collaborate with one another. With limited communication between companies, industry bodies, and governments, it can be difficult to understand the challenges and formulate the right responses. But by sharing intelligence and comparing notes on what works—and what doesn't—key players can mount a collective, concerted effort against their increasingly highly skilled adversaries.

Nations in Asia Pacific increasingly understand this need. For example, Singapore recently set up a dedicated OT cyber security information sharing and analysis centre (OT-ISAC) as well as sector-specific security operations centres (SOCs) to enable a shared understanding and coordinated response to critical infrastructure cyber threats. Read more in the Appendix: Highlights of resilience efforts in Asia Pacific.

Starting the journey

Now is the time to take action. Critical infrastructure operators need to establish integrated IT/OT cyber security programs backed by strong governance frameworks to protect essential services and public safety against mounting threats. At the same time, they need to overcome significant legacy challenges and plan for the future of essential services in Asia Pacific. The task may seem daunting at first, yet the right approach will lead to significant reduction in cyber risks while enabling service optimisation and the expansion of business initiatives. Here are six steps that organisations can start taking today to build cyber security into critical infrastructure.

1 Set the tone: Educate your stakeholders	• engage management and leadership by asking the right questions, and showcasing high-risk vulnerabilities and threat scenarios that directly impact operations.
2 Define the problem: Understand your unique landscape	• identify applicable laws and regulations • scope your mission-critical assets at the site and system levels • map cyber threats to your operations and assets.
3 Know where you stand: Evaluate and communicate your risk	• assess the maturity of your IT and OT cyber capabilities • identify the key gaps that require prioritised cyber investment • share the results with leadership.
4 Set your target: Define your framework	• identify key controls and clarify how they should apply to assets based on their nature and criticality • define your target governance and operating models.
5 Gear up: Develop your strategy	• identify high-yield priority initiatives from quick wins to transformative activities • develop your implementation roadmap supported by a risk-based transformation program • get boardroom buy-in.
6 Pilot and roll out: Start small, align, and scale	• pilot the changes, starting with non-intrusive controls at one or more representative sites; adjust designs and plans • phase roll-out across other critical assets.

A pragmatic, step-by-step approach focused on critical assets and high-yield initiatives—managed through a program with risk-reduction key performance indicators—will allow organisations to zero in on what matters and make the case for a bold transformation towards cyber resilience. That case can be greatly facilitated by involving stakeholders, from the board to field operations, early on, and presenting cyber resilience as a business issue that enables operational safety and reliability as well as value creation. In turn, this will help pave the way for greater efficiency, innovation, and new revenue streams that will benefit the organisation as a whole.

Conclusion

The digital revolution shows no signs of slowing down, especially in Asia Pacific, as critical infrastructure sectors and other industries embrace technologies such as IIoT and predictive maintenance analytics, along with the ongoing convergence of IT and OT. These technologies and trends unlock vast possibilities and benefits such as improved reliability and efficiency, but they also increase organisations' vulnerability to cyber threats.

The diversity of economies, geopolitical risk, and technology in Asia Pacific are reflected in the disparity in the maturity and enforcement of cyber security requirements in critical infrastructure. While some locations have laws or regulations in place, these often focus on risk management and supervisory powers. More enforcement of specific standards and technical requirements for critical industrial environments is needed.

Nevertheless, awareness of cyber threats to these environments is growing. Critical infrastructure operators are observing cyber attacks with severe impacts among their peers in Asia Pacific and globally, and now understand that the question of their operations being compromised is not a matter of "if" but "when". From governments to organisations, the region is quickly ramping up its efforts to secure critical infrastructure with a shift towards the adoption of internationally recognised cyber security standards and sector-specific maturity models, increased oversight, and information sharing.

Many organisations are just now starting their journey while some are still contemplating the best path forward. Yet the growing sophistication and potency of today's threats, along with the increasing exposure of vulnerable OT systems, highlights the urgency of addressing these challenges and developing robust and pragmatic cyber security programs focusing on both IT and OT environments. Without such programs, the operation of our critical infrastructure—on which the functioning of our societies and our economies depend—is not guaranteed.

Not all critical infrastructure organisations are the same; each industry and indeed each organisation will have its own unique cyber security requirements. However, every organisation will benefit from building a program based around people, process, and technology. And these benefits will only multiply with further collaboration. By sharing our insights and experiences within and across sectors and geographies, we can work together towards greater resiliency of the essential services underpinning society.

Appendix: Highlights of resilience efforts in Asia Pacific

Asia Pacific nations are varied in their approach to managing cyber threats to their critical infrastructure and operations. A few have long-standing security initiatives and regulatory frameworks to drive cyber resilience, others do not yet have strong enforcement systems in place, while many are just getting started with their efforts to address risks to mission-critical operational environments and systems.

Below we present highlights of efforts from several Asia Pacific locations, focusing on current laws, regulations, and supervisory frameworks applying to OT cyber security in critical infrastructure across essential public and private industries.

Australia

The Australian government created its Critical Infrastructure Centre[19] in 2017 and introduced regulatory frameworks applying to the telecommunications, electricity, gas, ports, and water sectors through the Telecommunications and Other Legislation Amendment Act 2017[20] and the Security of Critical Infrastructure Act 2018.[21] The issue is therefore at the top of the agenda for most critical infrastructure organisations' Chief Information Security Officers, Chief Executive Officers, and boards. They, and their organisations, can take advantage of several helpful initiatives to gain insight into the cyber security of their critical infrastructure.

The Australian Energy Market Operator, for example, recently developed the Australian Energy Sector Cyber Security Framework,[22] which leverages the ES-C2M2 framework and aims to give operators a better understanding of their current cyber security environments as well as the tools to mature those environments. Although the framework is largely directed at energy companies, organisations in other industries, such as water utilities, have also found it useful.

The federal government is taking other steps to increase risk awareness and boost incident support by giving all Australian companies access to helpful resources from organisations such as the Australian Cyber Security Centre[23] and the Attorney-General's Trusted Information Sharing Network.[24] The Australian Signals Directorate has also developed and published a set of strategies to help critical infrastructure owners mitigate the impacts of cyber security incidents.[25] Known as the "Essential Eight", these strategies are being adopted by the nation's major critical infrastructure providers.

Some sectors are also implementing major international standards such as ISA/IEC 62443 to help manage cyber threats to their OT assets.

China

In Chinese mainland, cyber security is principally governed by the Ministry of Industry and Information Technology (MIIT), which collaborates with the Public Security Bureau (PSB) and the Cyberspace Administration of China (CAC) to develop and enforce cyber security policies and regulations. The MIIT and PSB released administrative regulations to enforce IT and OT cyber security practices, especially for organisations regarded as providing critical information infrastructure. A key technical standard released for OT cyber security in all industries is the ICS extension of the broader Classified Protection of Cybersecurity 2.0 (CPCS) issued in 2019. The CPCS 2.0 supports China's broader Cyber Security Law,[26] which took effect in 2017 and outlines general compliance requirements for all public and private organisations in China.

Chinese critical infrastructure operators are widely following these standards and other emerging laws and regulations, setting up centralised governance mechanisms, and adopting the ISA/IEC 62443 standards and NIST SP800-82 guidelines to better protect their operations.

India

The Information Technology Act 2000 (amended 2008)[27] and the Information Technology Rules 2013[28] regulate organisations' cyber security in India. The Information Technology Act states that the government may define any computer resource that supports or relates to the operation of critical infrastructure as a protected system.

Critical infrastructure organisations in multiple sectors such as power and utilities, telecommunications and transport, and strategic and public enterprises operate according to the Guidelines for the Protection of National Critical Information Infrastructure[29] issued by the National Critical Information Infrastructure Protection Centre (established in 2014). These guidelines cover the entire cyber security lifecycle including planning, implementation, operations, disaster recovery, and business continuity planning, as well as reporting and accountability.

Japan

The Basic Act on Cyber Security 2014[30] is Japan's key law that sets principles, objectives, and government responsibilities for cyber security. The Basic Act also established the Cybersecurity Strategic Headquarters, which in 2015 reorganised the existing National Information Security Center as the National center of Incident readiness and Strategy for Cybersecurity (NISC).[31] NISC took on the primary responsibility for developing and coordinating cyber security policy across the public and private sectors, with a dedicated subgroup on Critical Infrastructure Protection.

In April 2017, the Cybersecurity Strategic Headquarters published NISC's fourth edition of the Cyber Security Policy for Critical Infrastructure Protection.[32] Maintaining the purpose of its predecessor policies—the protection of critical infrastructure—the policy gives both industry and government a cyber security framework within which to work. It focuses on five key improvement areas: cyber security measures, information sharing, incident response, risk management and incident readiness, and promotion. NISC followed up with the fifth edition of its Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure,[33] which details the cyber security measures to be adopted by critical infrastructure operators and related entities, and a guide and toolkit for conducting risk assessments.

Macau SAR

The Macau Cybersecurity Law (MCSL)[34] came into force in December 2019. With this law, public and private operators of critical infrastructure within the Macau Special Administrative Region have to meet obligations that aim to protect their information networks, computer systems, and control systems. The scope of the MCSL includes organisations in sectors such as utilities and transportation, which use OT, IoT, and other smart technologies. See Deloitte's report, *Macau Cyber Security Law (MCSL) – General Introduction and Impact Analysis*,[35] to obtain more understanding on the MCSL's regulatory requirements.

New Zealand

New Zealand's National Cyber Security Centre collaborated with the New Zealand Control Systems Security Information Exchange to develop voluntary standards for OT security with a primary focus on the electricity system and other critical infrastructure organisations. The latest version was released in 2019 as the Voluntary Cyber Security Standards for Control System Operators,[36] which draws from the NERC CIP standards and NIST guidelines such as the NIST CSF. The government previously released the Voluntary Cyber Security Standards for Industrial Control Systems in 2013.[37]

These guidelines are voluntary, but they may become mandated standards in the future. As a result, some critical infrastructure operators are leveraging the guidelines as a reference for their own cyber security frameworks.

Singapore

While the Cyber Security Act 2018[38] regulates cyber security in Singapore in general, the Cybersecurity Code of Practice (CCoP) for Critical Information Infrastructure Systems[39] specifically regulates security practices in critical infrastructure industries. To comply with the code, companies in these industries follow the security frameworks set out in ISA/IEC 62443, NIST SP800-37,[40] NIST SP800-30,[41] and RISK IT.[42]

The Cyber Security Agency of Singapore (CSA) followed up with the 2019 Operational Technology Cybersecurity Masterplan,[43] which presents a multifaceted strategy for both public and private organisations. The strategy focuses on:

- developing and coordinating specialised OT cyber security training
- setting up a dedicated OT cyber security information sharing and analysis centre (OT-ISAC) as well as sector-specific security operations centres (SOCs)

- driving OT cyber security innovation through public private partnerships.

In addition, the CSA worked to strengthen the aforementioned CCoP by adding mandatory requirements specifically tailored to OT environments. With this bold plan, the government aims to quickly develop and strengthen the critical infrastructure ecosystem's cyber resilience by increasing awareness of threats and challenges; enabling and promoting cyber security practices and solutions; enhancing collaboration; driving and streamlining initiatives; and supporting organisations in their OT cyber security journeys.

The launch of this masterplan is expected to further drive critical infrastructure organisations' efforts on OT cyber security, after having been set on a compliance path by recently enacted legislation and mandatory guidelines such as the CCoP.

South Korea

The Act on the Protection of Information and Communications Infrastructure 2001[44] (amended 2019)[45] regulates cyber security in many of South Korea's critical infrastructure sectors, including national security, administration, public security, defence, finance, communications, transportation, and energy. The 2019 amendment grants additional powers for central authorities to order inspections of organisations deemed to operate critical information and communications infrastructure (CII organisations). According to the Act, CII organisations shall formulate and implement cyber capabilities such as intrusion prevention, backup, and restoration. These are defined as the "Measures to protect critical information and communications infrastructure", which are reviewed on a yearly basis by the Ministry of Science and ICT (MSIT) and government agencies, based on periodic identification of CII organisations and inspections of their cyber security posture. Vulnerability assessment checklists are also made available to support organisations and government agencies conducting inspections.

South Korea's CII organisations generally consider the "Measures to protect critical information and communications infrastructure", the Korea Internet & Security Agency Information Security Management System, and the NIST CSF as three of the main cyber risk management frameworks. Energy companies also apply ISO/IEC 27019:2017,[46] which is based on ISO/IEC 27002:2013,[47] to their process control systems. This standard provides cyber security guidance for the production, generation, transmission, storage, and distribution of electricity, gas, oil and heat, and on managing supporting processes.

In the future, critical infrastructure operators are expected to start using ISA/IEC 62443 as a reference framework for developing cyber security practices. For example, the chemicals sector will likely leverage these standards to protect OT and IIoT while implementing smart factory concepts in their production facilities. Telecommunications companies are also exploring their cyber security options as they develop 5G deployment strategies.

Taiwan

The Executive Yuan of Taiwan published its Guidelines for National Critical Infrastructure Protection in 2014.[48] For protection against general risks, critical infrastructure companies in Taiwan regard this policy as their main guiding framework. Although the guidelines cover a wide range of risks, cyber security is their focal point. In 2018, the Executive Yuan published its Recommendations for Cybersecurity Protection of Critical Information Infrastructure,[49] which focuses largely on OT environments.

In addition to these guidelines, two cyber security laws and regulations apply to most public sector and critical infrastructure organisations in Taiwan: the Cyber Security Management Act 2018[50] and the Enforcement Rules of Cyber Security Management Act.[51] Six additional draft regulations supporting the Cyber Security Management Act have been released for public review and comment.

To comply with these acts, some critical infrastructure operators in Taiwan leverage existing guidelines, standards, and frameworks referenced by the Executive Yuan in its publications, such as NIST SP800-82, ISA/IEC 62443, NERC CIP, and the US Nuclear Regulatory Commission's Regulatory Guide RG5.71.[52]

Endnotes

1. Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011.
2. Deloitte Insights, *The Fourth Industrial Revolution: At the intersection of readiness and responsibility*, 2020.
3. Repository of Industrial Security Incidents (RISI) Database, "Steel plant infected with Conficker," accessed March 18, 2020.
4. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018; Deloitte, "All hands on deck: Supporting Maersk as it recovers from a global cyber attack," accessed March 25, 2020.
5. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016.
6. Nicole Perlroth and Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.," *The New York Times*, March 15, 2018.
7. GlobalData, "Asia-Pacific will lead 5G technology adoption by 2024, says GlobalData," January 13, 2020.
8. ABI Research, *Critical Infrastructure Protection (CIP) Market Size, Share & Trends Analysis Report By Security Type (OT, IT), By Services (Consulting, Risk Management, Managed), By Application, And Segment Forecasts, 2018 - 2025*, 2018.
9. Ibid.
10. International Society of Automation, "New ISA/IEC 62443 standard specifies security capabilities for control system components," accessed February 20, 2020.
11. National Institute of Standards and Technology, "Cybersecurity Framework," accessed March 24, 2020.
12. Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn, "Guide to Industrial Control Systems (ICS) Security," *NIST Special Publication* 800-82 Revision 2, May 2015.
13. North American Electric Reliability Corporation, "CIP Standards," accessed March 18, 2020.
14. Office of Cybersecurity, Energy Security, And Emergency Response, "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)," accessed March 18, 2020.
15. Dragos, "Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas," June 14, 2019.
16. Greenberg, "The Untold Story of NotPetya"; Deloitte, "All hands on deck".
17. Nick Hunn, "How to Hack a Smart Meter and Kill the Grid," October 8, 2018.
18. Reuters, "S. Korea accuses North of hacking railway systems and officials' phones," March 8, 2016; Jacqueline O'Leary & al., *Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware*, FireEye, September 20, 2017; Utpal Bhaskar, "India's power industry comes under increasing cyberattacks from hackers," *Livemint*, September 11, 2019; Dragos, "Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas," June 14, 2019; Binayak Dasgupta and Sudhi Ranjan Sen, "Cyber attack at Kudankulam; critical system safe," *Hindustan Times*, October 30, 2019.
19. Critical Infrastructure Centre, "Critical Infrastructure Centre," accessed March 18, 2020.
20. Critical Infrastructure Centre, "Telecommunications Sector Security," accessed March 18, 2020.
21. Critical Infrastructure Centre, "Security of Critical Infrastructure Act 2018," accessed March 18, 2020.
22. Australian Energy Market Operator (AEMO), "AESCSF framework and resources," accessed March 22, 2020.
23. Australian Cyber Security Centre, "Australian Cyber Security Centre," acessed March 22, 2020.
24. Trusted Information Sharing Network, "Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience," accessed March 5, 2020.
25. Australian Cyber Security Centre, *Essential Eight Explained*, April 2019.
26. Deloitte, "A new era for Cybersecurity in China," accessed March 10, 2020.
27. Ministry of Electronics & Information Technology, "Information Technology Act 2000," accessed March 18, 2020.
28. The Indian Computer Emergency Response Team, *Information Technology Rules 2013 (CERT-In Rules)*, January 16, 2014.
29. National Critical Information Infrastructure Protection Centre (NCIIPC), *Guidelines for the Protection of National Critical Information Infrastructure*, January 16, 2015.
30. Ministry of Justice, "Basic Act on Cybersecurity," November 12, 2014.
31. National center of Incident readiness and Strategy for Cybersecurity, "About NISC," accessed March 10, 2020.

32. National center of Incident readiness and Strategy for Cybersecurity, *The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)*, April 18, 2017, (Revised July 25, 2018).
33. National center of Incident readiness and Strategy for Cybersecurity, *Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure (5th Edition)*, April 4, 2018.
34. Macau Special Administrative Region, "Cyber Security Law," 2019, accessed March 10, 2020.
35. Deloitte, *Macau Cybersecurity Law – General Introduction and Impact Analysis*, December 2019.
36. National Cyber Security Centre and the Control Systems Security Information Exchange, *Voluntary Cyber Security Standards for Control Systems Operators (VCSS-CSO)*, 2019.
37. Government Communications Security Bureau, *Voluntary Cyber Security Standards for Industrial Control Systems*, v.1.0., 2014.
38. Parliament of Singapore, *Cybersecurity Act 2018*, Bill No. 2/2018.
39. Cyber Security Agency of Singapore, "Cybersecurity Code of Practice for Critical Information Infrastructure," accessed March 12, 2020.
40. National Institute of Standards and Technology, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy – 2018," *NIST Special Publication* 800-37 Revision 2, December 2018.
41. National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," *NIST Special Publication* 800-30 Revision 1, September 2012.
42. Information Systems Audit and Control Association, *The Risk IT Framework*, June 30, 2010.
43. Cyber Security Agency of Singapore, *Singapore's Operational Technology Cybersecurity Masterplan 2019*, October 1, 2019.
44. Korea Law Translation Center, "Act on the Protection of Information and Communications Infrastructure," accessed March 15, 2020.
45. National Law Information Center, "Information and Communications Infrastructure Protection Act" (Korean only), accessed March 15, 2020.
46. International Organization for Standardization, "ISO/IEC 27019:2017 [ISO/IEC 27019:2017] Information technology — Security techniques — Information security controls for the energy utility industry," accessed March 24, 2020.
47. International Organization for Standardization, "ISO/IEC 27002:2013 [ISO/IEC 27002:2013] Information technology — Security techniques — Code of practice for information security controls," accessed March 24, 2020.
48. Homeland Security Police Committee, Executive Yuan, "Protection – Eliminate potential impacts and build resilience," accessed March 18, 2020.
49. National Information and Communication Security Taskforce, "Recommendations for Cybersecurity Protection of Critical Information Infrastructure," (non-official translation), 2018, accessed March 18, 2020.
50. Law and Regulations Database of The Republic of China, "Cyber Security Management Act," 2018, accessed March 24, 2020.
51. Michael R. Fahey, *A quick look at Taiwan's Cyber Security Management Act Enforcement Rules*, Winkler Partners, January 22, 2019.
52. US Nuclear Regulatory Commission, *Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities*, January 2010.

Authors and contributors

Authors

Max Y. Lin
Asia Pacific Cyber OT/ICS & IoT leader
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

Etienne Janot
Senior manager
+886 2 2725 9988 (ext. 7766)
etjanot@deloitte.com.tw

Key contributors

Karen Grieve
Director
+61 2 9322 7321
kagrieve@deloitte.com.au

Bill Hsiao
Manager
+886 2 2725 9988 (ext. 7658)
bihsiao@deloitte.com.tw

Tommy Thompson
Senior manager
+61 8 9365 7185
phthompson@deloitte.com.au

Acknowledgements

We wish to thank the following Deloitte people for their contributions to this report.

Matthew Holt
Global Cyber OT/ICS & IoT leader
+39 049 792 7998
maholt@deloitte.it

We would also like to thank Jeff Campbell, CISO at Horizon Power, for sharing his experience.

Key contacts

James Nunn-Price
Asia Pacific Cyber leader
+61 428 200 542
jamesnunnprice@deloitte.com.au

Max Y. Lin
Asia Pacific Cyber OT/ICS & IoT leader
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

Australia

David R. Owen
Partner
+61 2 8260 4596
dowen@deloitte.com.au

Chinese Mainland/Hong Kong

Boris Zhang
Partner
+86 21 6141 1505
zhzhang@deloitte.com.cn

Eva Kwok
Partner
+852 2852 6304
evakwok@deloitte.com.hk

India

Gaurav Shukla
Partner
+91 80 6188 6164
shuklagaurav@deloitte.com

Japan

Haruhito Kitano
Partner
+81 803 591 6426
haruhito.kitano@tohmatsu.co.jp

Korea

Jaewoong Lee
Senior manager
+82 2 6676 2918
jaewoonlee@deloitte.com

New Zealand

Anu Nayar
Partner
+64 4 470 3785
anayar@deloitte.co.nz

Southeast Asia

Weng Yew Siah
Partner
+65 6216 3112
wysiah@deloitte.com

Taiwan

Max Y. Lin
Asia Pacific Cyber OT/ICS & IoT leader
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

Designed by CoRe Creative Services. RITM0413214

This is printed on environmentally friendly paper