Principles of operational technology cyber security

Content Complexity
MODERATE ● ● ○

Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

National Cyber Security Centre

a part of GCHQ

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

Te Tira Tiaki

Government Communications Security Bureau

National Cyber Security Centre

PART OF THE GCSB

Bundesamt für Sicherheit in der Informationstechnik

National Cyber Security Centre

Ministry of Security and Justice

NISC 内閣サイバーセキュリティセンター

National center of Incident readiness and Strategy for Cybersecurity

警察庁

National Police Agency

This publication was developed by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) in collaboration with the U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing and Analysis Center (MS-ISAC), United Kingdom's National Cyber Security Centre (NCSC-UK), Canadian Centre for Cyber Security (Cyber Centre), New Zealand's National Cyber Security Centre (NCSC-NZ), Germany's Federal Office for Information Security (BSI Germany), the Netherlands' National Cyber Security Centre (NCSC-NL), Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and National Police Agency (NPA), and the Republic of Korea's National Intelligence Service (NIS) and NIS' National Cyber Security Center (NCSC).

Contents

Introduction

Critical infrastructure organisations provide vital services, including supplying clean water, energy, and transportation, to the public. These organisations rely on operational technology (OT) to control and manage the physical equipment and processes that provide these critical services. As such, the continuity of vital services relies on critical infrastructure organisations ensuring the cyber security and safety of their OT.

Due to the extensive integration of OT in the technical environments of critical infrastructure organisations, and the complex structure of these environments, it can be difficult to identify how business decisions may affect the cyber security of OT, including the specific risks attributed to a decision. Decisions may include introducing new systems, processes, or services to the environment; choosing vendors or products to support the technical environment; and developing business continuity and security-related plans and playbooks. This document is designed to assist organisations make decisions for designing, implementing, and managing OT environments to ensure they are both safe and secure, as well as enable business continuity for critical services.

Principles of OT Cyber Security, authored by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), and co-sealed by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing and Analysis Center (MS-ISAC), United Kingdom's National Cyber Security Centre (NCSC-UK), Canadian Centre for Cyber Security (Cyber Centre), New Zealand's National Cyber Security Centre (NCSC-NZ), Germany's Federal Office for Information Security (BSI Germany), the Netherlands' National Cyber Security Centre (NCSC-NL), Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and National Police Agency (NPA), the Republic of Korea's National Intelligence Service (NIS) and NIS' National Cyber Security Center (NCSC) describes six principles that guide the creation and maintenance of a safe, secure critical infrastructure OT environment:

1. Safety is paramount
2. Knowledge of the business is crucial
3. OT data is extremely valuable and needs to be protected
4. Segment and segregate OT from all other networks
5. The supply chain must be secure
6. People are essential for OT cyber security

The principles have been co-designed with Australian critical infrastructure operators. We thank all who have contributed for their time and expertise in supporting the development of this document.

How to use this document

The authoring agencies recommend an OT decision maker apply the six principles presented in this document to help determine if the decision being made is likely to adversely impact the cyber security of the OT environment. If a decision impacts or breaks one or more of the principles of OT cyber security outlined in this document, then it will likely introduce a vulnerability to the OT environment. Such a decision therefore needs to be examined more closely to make sure the right cyber security controls are put in place and that the residual risk after the controls are put in place is acceptable, or, alternatively, the proposal is reconsidered. Quickly filtering decisions to identify those that impact the security of OT will enhance the making of robust, informed, and comprehensive decisions that promote safety, security and business continuity when designing, implementing, and managing OT environments.

The authoring agencies recommend OT decision makers read and understand each principle. This document is intended to be useful for all personnel who need to filter decisions affecting OT, from the leadership of an organisation (including the executives and board members making strategic decisions) down to the technical personnel making tactical and operational decisions.

Principles of operational technology cyber security

Principle 1: Safety is paramount

Safety is critical in physical environments. In contrast to corporate IT systems, where leaders prioritise innovation and rapid development without concern of threat to life, operational cyber-physical systems' leaders must account for threat to life in daily decision making. First-order hazards from critical infrastructure include high voltages, pressure releases or flammable explosions, kinetic impacts (e.g, speeding trains), and chemical or biological hazards such as in water treatment. Further, there are implications for citizens' way of life if essential services such as energy and drinkable water supply are degraded or disrupted. The interconnected nature of critical infrastructure means that failures, whether by human error or malicious disruption through cyber means, may have wide ranging and unforeseen implications for the day-to-day function of society.

Examples and implications

When discussing safety, it may be useful to consider safety of human life; safety of plant, equipment and the environment; and the reliability and uptime of the critical infrastructure's services. Depending on the environment and the system being considered, this may imply a requirement that any cyber security systems, processes and services introduced into the environment are deterministic and predictable, including that engineers have a deep understanding of the weaknesses of the system and ensuring that failures occur in an expected and manageable way. Similarly, safety needs to be informed by cyber security and an understanding of the threat environment. Depending on the criticality of the service, there may be a need to ensure that any cyber security systems, processes or services introduced into the environment are black-start compliant, meaning they will not hinder a restart after a complete loss of electricity, and are able to operate and recover with minimal dependence on other systems.

The principle of "safety is paramount" implies the following incident response questions are significant:

- If there is a cyber incident in an area that requires software running correctly for the work environment to be considered safe (safety and protection systems), is an organisation prepared to send staff to that site knowing that a bad actor has been, or is currently, on the network?

- If there is a cyber incident in an area that requires software running correctly for the work environment to be considered safe (safety and protection systems), in many instances this means that paying a ransom cannot be an option, as there is no timely large-scale method to verify that the system has been returned to a safe state. Can an organisation be confident that the encryption process was the only modification to the files, given that a malicious actor is known to have been on the OT network?[1]
- Is restoring from backup an acceptable approach to mitigate cyber incidents? That is, if a malicious actor has been on the network for a period of time, can the backups be trusted? Is there a way to validate that the critical OT system is safe, after recovery?

Safety of human life, safety of the plant equipment, safety of the environment, and the need to maintain reliability and uptime, are necessary systemic ways of thinking that need to permeate all tasks, even essential and common cyber hygiene tasks potentially considered unrelated, such as:

- How to take a backup? Are there risks to executing backups over the same (potentially close-to-saturated) network as time-critical safety control messages?
- How to do asset discovery? Are active processes acceptable, or is passive the only way?
- How to patch, and how to do change management in general? What are the system requirements for frequency, testing rigour, scope, roll-out strategies and roll-back strategies.

Principle 2: Knowledge of the business is crucial

The more knowledge a business has about itself, the better that business can protect against, prepare for and respond to a cyber incident. The higher in the organisation there is understanding, visibility and reporting of cyber risks, especially to OT systems, the better the outcome.

All critical infrastructure organisations should ensure they meet the following baselines:

- Identify the vital systems the organisation needs to continue to provide their crucial services
- Understand the OT system's process, and the significance of each part of the process
- Create an architecture that allows those vital systems and processes to be defended from other internal and external networks
- Ensure that personnel responsible for designing, operating and maintaining OT systems understand the business context that the OT system operates within, including the physical plant and process connected to the OT system and how it delivers services to stakeholders.
- Understand the dependencies vital systems have to be able to operate and where they connect to systems external to the OT system.

1 Note ASD ACSC's advice is never pay a ransom. See our guidance on how to report and recover from ransomware - https://www.cyber.gov.au/report-and-recover/recover-from/ransomware

Examples and implications

A commonly agreed upon imperative of cyber security is to know what needs to be protected. The first part of this is to understand which elements of the business are essential for the organisation to be able to provide its critical services. The second part is to understand the systems and processes being protected. This may include (but is not limited to): systems engineering drawings, asset lists, network diagrams, knowing who can connect to what and from where, recovery procedures, software vendors, services and equipment, and, to the extent possible, software bills of material and the desired configuration state.

Knowing what parts of the business are essential to be able to provide a critical service requires both top-down and bottom-up thinking. Top-down thinking has historically led many organisations to seek to separate OT from IT. Bottom-up thinking provides an opportunity for an organisation to go further and discover the minimal set of OT equipment required for a critical function. For example, to be able to generate electricity, depending on the generator, it may be that the minimum requirement is the generator, a controller in a control panel, and a suitable fuel supply. For critical infrastructure entities, understanding what is needed to protect the absolute core functions – keeping the water flowing and the lights on – should then guide the effective layering of cyber security controls. This has implications for architecture, protection, detection, and backup of devices and files.

It is essential that OT-specific incident response plans and playbooks are integrated into the organisation's other emergency and crisis management plans, business continuity plans, playbooks and mandatory cyber incident reporting requirements. The involvement of a process engineer is important, both when creating plans and playbooks and during any investigation, containment or recovery processes. There is also a need to provide an information pack to third parties before or when they are engaged, to quickly bring them up to speed. This third-party pack should include the likes of points of contact, naming conventions for servers, data sources, deployed tools, and what tools are acceptable to be deployed. All plans, playbooks, and third-party packs must be regularly exercised, updated by all relevant parties including legal, and protected due to their value to the adversaries.

Physical aspects that aid staff to have knowledge of the OT system should also be considered. This may include colour coding cables, putting coloured banding on existing cables, or marking devices allowed in the OT environment in a highly visible way. Only authorised devices should be connected to the OT environment, to help ensure that only authorised code can be introduced to OT environments. Overt visual cues allow an organisation to better protect their environment by identifying unauthorised devices, and allow an organisation to quickly make correct decisions in response to cyber or intelligence-based events. Such markings would need to be periodically assessed and verified to ensure accuracy and currency.

Understanding the business context of the OT system is essential for assessing the impact and criticality of OT outages and cyber security compromises. It is also vital to determining recovery priorities during a critical incident. For organisations reliant on OT to be able to provide a critical service, an integrated OT cyber security function is a necessary part of the business. OT cyber security personnel are not expected to have the deep understanding of a physical system that an electrical, chemical, or process engineer may have, but they should have a working knowledge of plant operation and most importantly, maintain working relationships with those in the organisation responsible for the physical plant. Such relationships are critical both to the success of any cyber enhancement project as well as when there is a need to respond to a cyber event.

Principle 3: OT data is extremely valuable and needs to be protected

From an adversary's point of view, knowing how a system is configured, including devices and protocols used, is valuable since an OT environment rarely changes. This level of information allows a bad actor to create and test targeted malware, facilitating a greater range of possible malicious outcomes.

Of particular importance is engineering configuration data, such as network diagrams, any documentation on the sequence of operations, logic diagrams and schematics (e.g., the knowledge that address 1250 is a circuit breaker, or understanding the organisation's DNP3 address convention for devices of a specific type). This information is unlikely to change in five years, and may last for 20 or more years. As such, engineering configuration data has enduring value and is highly valuable to an adversary. An adversary gaining in-depth knowledge of how an OT system works may be likened to the concept of prepositioning in a corporate IT environment, particularly in the sense of significance and the need to respond.

Also important is more ephemeral OT data, such as voltage or pressure levels, as it can provide insight into what the organisation or its customers are doing or how the control system works. Securing OT data is also important for the protection of intellectual property (IP) and personally identifiable information (PII), such as for metering in electricity, gas or water, or for patient records in health. These other types of OT data, such as ephemeral OT values, IP and PII, also need to be protected. However, OT personal should also protect the engineering configuration data, which is critical to operations and valuable to malicious actors, but often overlooked.

Examples and implications

Organisations should define and design where and how OT data can be stored, so as to control and secure it. While OT systems are often segmented and segregated from corporate IT systems, frequently adversaries do not need to access the more highly protected OT systems to gain access to all necessary OT data. Organisations may need to change their business processes to minimise the distribution and storage locations of OT data, including internally to the corporate system, such as processes that require that staff store OT configuration files in the corporate document management system. Ideally, critical OT data is always protected to the level of the OT system and as such should be stored in a protected repository that is segmented and segregated from the corporate environment and the internet.

OT networks should push data out of the network, rather than external networks pulling data in from OT.

When seeking to identify where critical OT data is, indicative questions include:

- Do vendors and service technicians have a copy?
- Do consultants have a copy?
- Do engineers work in corporate IT systems, which allows them to correspond with other experts via email, before transferring the work to the OT environment?
- Is the data stored in emails, laptops, corporate backup devices, or in the cloud?
- What is the process for information destruction and disposal (e.g., when a programmable logic controller (PLC) is decommissioned, is the logic code wiped)?

- Is there anything to prevent technologies such as endpoint detection and response (EDR) or anti-virus causing an inadvertent data spill by sending copies of OT files out of the organisation's network? Is there anything to prevent staff from uploading files to online antivirus or storage services?
- How much information is shared with the insurer, HR, procurement, social media, etc.?
- Where are OT log files stored and analysed?
- Are usable solutions in place, so that all parties working in OT do not have to create workarounds, potentially saving information in inappropriate places just to complete their work?

Organisations should seek to do more than protect the confidentiality, integrity and availability of OT data. Ideally they are alerted when OT data is viewed or exfiltrated – potentially via implementing canary tokens, which may include responses on certain files if they are touched. Further, they should consider what data adversaries already have access to, and if that data can be changed. This includes default passwords. If default passwords are changed, ideally ensure there is a way to capture failed login attempts, and investigate them.

Principle 4: Segment and segregate OT from all other networks

Segmenting and segregating more critical functions and networks has been common advice for decades. That advice is covered in many prior publications[2]. Entities should segment and segregate OT networks from the internet and from IT networks, because the corporate IT network is usually assessed as having a higher risk of compromise due to its internet connectivity, and services like email and web browsing. We add to, rather than change, prior advice in two main areas.

"From all other networks"

The first additional area relates to the need to secure connections between the critical infrastructure organisation's OT network and other organisations' OT networks. These connections from other organisations' OT networks can be a backdoor into a critical asset, potentially bypassing levels of security protecting the OT network from corporate IT, and the internet.

Critical Infrastructure organisations should segment and segregate their OT from all other networks. Fairly well understood in recent times is the need to protect and restrict OT networks from vendors. Also well understood since 2017's Hatman malware, is the need to separate more critical OT networks such as those essential to safety, from less critical OT networks. Less well understood is the need to protect and restrict OT networks from peers and services upstream and downstream, as defined in the example below.

2 Such as https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/network-hardening/implementing-network-segmentation-and-segregation, NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/0/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF, Stop Malicious Cyber Activity Against Connected Operational Technology https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/0/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF, and https://www.cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-version-20-itsp80022

Examples and implications

For example, an electricity transmission company may have connections between its own OT networks and the OT networks of other electricity transmission companies (peers). The electricity transmission company may also have a connection between its OT network and the OT networks of electricity generators (upstream). The electricity transmission company may have a connection between its OT network and the OT network of electricity distribution companies and large customers (downstream).

Compounding the long-standing issue of OT interconnectivity between different organisations is the disruption taking place in many critical infrastructure subsectors. As an example, in the electricity generation subsector, large monolithic generators are being replaced with many smaller generators and storage devices. The organisations running these smaller generators and storage devices may have overseas control rooms, and permanent connections from their OT networks to overseas vendors.

An important shift in thinking from engineering reliability to cyber security is the concept that if a connection exists, it needs to be secure, regardless of the size of the organisation it is connected to. That is, from an engineering reliability point of view, a connection to a 2GW power station is more critical than a connection to a 5MW solar farm. However, from the cyber security point of view of an attack vector into an electricity transmission organisation's OT network, a network connection to the control system of a 5MW solar farm has the same criticality as a network connection to the control system of the 2GW power station.

Organisations cannot presume that other organisations have the same cyber risk appetite, cyber hygiene and cyber security standards as their own. If an organisation's OT network is not sufficiently protected from another organisation's OT network, including usual considerations such as logging and alerts, then the security boundary for the OT network includes the other organisation. Understanding third-party risks is critical.

Segmentation within an OT network must be used where assets and processes have different levels of criticality or the environment has a different level of trust. For example, pole-top infrastructure in an electricity distribution network may only be secured with a padlock and may use untrusted cellular networks. This infrastructure should have a lower level of trust and be segregated from infrastructure in a zone substation that is protected with robust security measures and fully encrypted communications paths.

Administration and management

This principle also builds on advice surrounding the administration and management of OT systems and services. Typical advice involves segmenting and segregating OT networks from IT networks, logically and physically. In addition to this, organisations should explicitly consider where system administration and management services are placed, and ensure adequate separation of the administration and management interfaces from their IT environment counterparts. Compromise of the management and administration accounts or systems compromises the systems that they manage. Critical OT systems should not be reliant on IT systems to operate.

Examples and implications

A firewall is often placed between a corporate IT network and an OT network, because the corporate IT network is usually seen as having a higher risk of compromise. However, a common goal of malicious cyber actors, once on a network, is to seek privilege escalation. If a malicious cyber actor compromises the corporate IT network and achieves privilege escalation, and the firewall is managed from the IT side via a privileged IT account, then the firewall between IT and OT may no longer provide the desired level of protection for the OT environment. This architecture is always required when there are two environments of different trust and security levels: a more critical environment should never be administered from a less critical environment, and should always be managed from a network with the same or higher security posture.

There are many other instances where administration and management systems are critical, and hence require appropriate segmentation. For example, as noted by Microsoft, Active Directory (AD) Domains do not function as security zone boundaries inside an AD Forest. If the OT environment is inside the same AD Forest as the IT environment, or if a trust relationship exists, then the desired level of protection and operational separation for the OT environment may not be provided.

Similarly, virtualisation is becoming common in many OT environments. Consider the case where virtualisation of the OT infrastructure or components is managed by privileged accounts from a corporate domain. If the corporate environment becomes compromised, through ransomware or other mechanisms, even if the virtualised OT environment has not been directly affected, the privileged IT accounts required to manage the OT environment would be no longer accessible.

Another example of significance is backups. If the backups or backup infrastructure for the OT environment is managed by privileged corporate IT accounts, then again the desired level of risk mitigation against a cyber-incident may not be provided.

Segmenting and segregating networks has long been recommended as one of the primary ways of reducing cyber risk in OT environments. In addition to more traditional physical and logical separation concerns, administration and management systems are highlighted. As demonstrated by the above non-exhaustive list of vital administrative and management areas including network security, authentication and access control, virtualisation and backups, there is a need for organisations to regularly assess the risk of insufficiently separating administrative and management systems and services in OT environments.

Principle 5: The supply chain must be secure

Making supply chains more secure has been a focus of advice for some time. That advice is covered in many prior and current publications, including the need to have a supply chain assurance program for suppliers of equipment and software, vendors and managed service providers (MSPs), particularly when they have access to OT to provide support. The requirement to make supply chains more secure has often resulted in a level of rigour assessing major vendors in an organisation's OT environment. While organisations should still follow existing advice, we call out some additional areas of particular concern for OT environments.

Examples and implications

A shift in thinking is required regarding criticality and risk exposure presented by vendors. Organisations should re-evaluate the scope of systems that require oversight, as historically often only large vendors or vendors that are the most significant from an engineering point of view were scrutinised. For cyber security, size and engineering significance often does not matter.

In OT environments, the network is typically fairly open. Critical control messages are commonly sent with little or no security, such as without encryption. Some control systems protocols communicate via multicast or broadcast messages, which are sent to all devices on the network. As such, almost any device on the network may be able to view critical control messages, and could create and inject messages to cause an undesirable action, making the supply chain of all devices critical.

"Any device" includes peripherals such as printers, networking and telecommunications equipment, as well as the more commonly considered remote terminal units (RTUs), human machine interfaces (HMIs), engineering workstations, historians, relays, intelligent electronic devices (IEDs) and controllers. Other systems may also need to be considered, depending on interconnections or the necessity for the other system to be functioning correctly for the OT to function correctly. These may include building management systems, air conditioning (HVAC), fire suppression systems, elevators, cameras and physical access control systems.

The source and provenance of all devices in the OT environment should be known. This includes any vendor or consultant laptop connecting to the OT network, which may be used to access otherwise explicitly prevented content such as email or web browsing. Consideration should be given regarding what other networks, such as a vendor's alternative customer, the devices have been connected to, and if those networks are at the same trust level as the OT network. This includes the case where networking or other devices from lower trust corporate IT networks are repurposed for use in higher trust OT networks.

A small technical check that most organisations can do while evaluating a device, is to plug the device in with a packet analyser capturing traffic, and check if the device unexpectedly attempts to communicate with a remote address.

Another shift in thinking required is to not only consider what a device is currently configured to do, which can be tested, but also consider what a device could do if its firmware or configuration was changed. This is particularly important if the device is constantly or occasionally connected to a vendor, who can update the firmware. To aid protecting against third-party interference, entities should ensure that firmware is received from a trusted location, is cryptographically signed, and that the signature is checked.

Vendors can increase risk to OT systems. A vendor request, habit or architecture that requires an organisation to break one or more of the principles of OT cyber security can increase the OT system's susceptibility to cyber attack. Such activity should count negatively for a vendor's cyber security maturity when assessing the suitability of their products or services. A common example is a license renewal process, that requires connections from critical parts of the OT network out to the internet. Other examples include direct connections between OT and the internet, bypassing remote access security architecture, as a means to allow the vendor to collect data, perform firmware updates, make configuration changes, or to perform any other form of remote servicing or support.

Principle 6: People are essential for OT cyber security

A cyber-related incident cannot be prevented or identified in OT without people that possess the necessary tools and training creating defences and looking for incidents. Once a cyber-related incident has been identified in OT, trained and competent people are required to respond.

A strong safety-based cyber security culture is critical to the on-going cyber resiliency of OT systems. There is a need for each organisation to reframe the requirements from these principles as workplace safety requirements, as opposed to cyber security requirements.

Staff, particularly field technicians and all other members of operating staff, are often the front line of defence and detection for an organisation.

Examples and implications

A mix of people with different backgrounds, with various skills, knowledge, experience and security cultures, is necessary to support effective OT cyber security practices. This includes members from infrastructure and cyber security teams (commonly found in IT), as well as control system engineers, field operations staff, and asset managers (commonly found in OT).

Developing a cohesive OT cyber security culture requires general alignment on the principles of OT throughout the organisation. Consider that there will be a different set of inherent values and priorities carried by members of different backgrounds. For example, the first principle of OT cyber security, "Safety is paramount", often requires a fundamental shift in thinking for people that have non-engineering or non-critical infrastructure backgrounds. Team members with non-engineering backgrounds gaining an understanding of OT challenges is important for the team to work cohesively in OT.

In most critical infrastructure OT sites, from electricity generation to water treatment facilities, staff are the front line of defence. They almost certainly will not be OT cyber security experts, nor people who work in corporate IT. Field operations staff rarely receive formal information technology or cyber security training and certification. Often, experience with the IT components of an Industrial Control System (ICS) will have been developed on-the-job, out of necessity due to the growing dependency of site operations on ICT infrastructure and IP-based communication.

As such, significant focus is required to develop cyber security awareness as a core component of field safety culture, so that operators feel confident and empowered to raise potential cyber concerns, without fear of ridicule or judgement. Further, there needs to be a process put in place where cyber-safety related observations can be raised quickly, with a culture of knowing that observations will be appreciated.

Potential strategies to develop security awareness and a cyber-safe culture amongst staff include:

- Incorporating cyber security into safety assessments, factory acceptance testing (FAT), site acceptance testing (SAT), and the engineering change management process. Established methods include Cyber-Informed Engineering, Cyber PHA or HAZCADS.
- Creating environments and processes that encourage local staff to identify and report suspicious behaviour. A common anti-pattern is for engineers to perform remote maintenance without informing on-site staff. The field operator will observe the engineer's activities as a mouse moving on a local machine or visible interaction with the HMI. Local staff will grow to ignore such behaviour as being normal and legitimate.
- Conditioning field operators to consider the possibility of cyber compromise when operational faults are identified. Historically, faults that engineers address have been due to engineering issues such as misconfiguration, device failure, corruption of data or the device working outside of tolerances. Typical responses include restarting the program, rebooting or resetting the device, re-flashing or loading a known good configuration, or replacing the device. Historically, malicious cyber actions have not been considered, meaning that cyber incidents may have been misidentified and dismissed as operational faults or missed entirely. The possibility that a fault has a cyber-related cause should also be considered. Most, if not all, of the traditional remediation steps listed will reset communication links and wipe volatile memory, which may have helped a cyber security investigation. Specific additional processes, and changes to long existing processes, are required for cyber identification, classification and investigations in OT.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre