WHITE PAPER

Six Steps to a Secure State for Critical Infrastructure Operators

Protecting the Nation's Critical Infrastructure With New Legislation

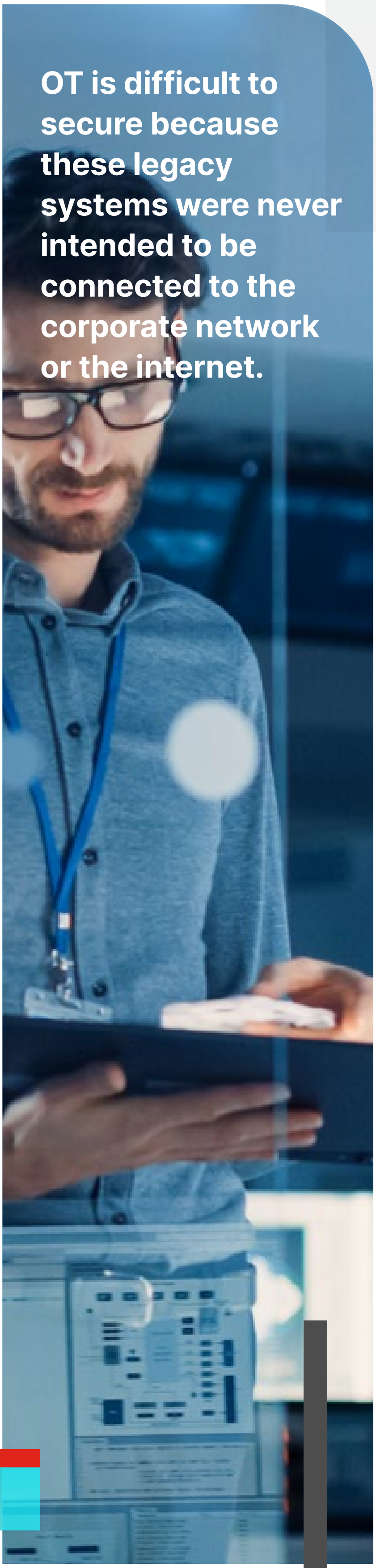
The Australian government is in the process of redefining which industries are included in the definition of the nation's critical infrastructure (CI). These industries are vital for the smooth running of Australian society and include electricity, gas, water, maritime ports operators, communications, financial services and markets, higher education and research, food and grocery, healthcare, transport, and water treatment, among others.

Disruption to the provision of goods and services delivered by CI operators in any of these sectors could cause significant real-world repercussions, ranging from inconvenient to catastrophic. For example, a cyberattack on transport systems could cause traffic delays (inconvenient) or accidents (potentially life-threatening). Or, if cyberattackers were able to sabotage the water treatment system, Australia's drinking water could become poisoned.

The Australian government has introduced the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (Cth), which includes requirements for organisations in these industry sectors to strengthen their cybersecurity protections. The *Critical Infrastructure Bill* will require CI operators to demonstrate that they have developed and maintained a CI risk management program and to report serious cybersecurity incidents.[1]

This may seem simple on the surface since information technology (IT) cybersecurity tools are widely available in the marketplace and the threat landscape is relatively well understood. However, securing CI assets is a different proposition than securing IT networks due to the unique nature of the operational technology (OT) that underpins CI assets.

OT is difficult to secure because these legacy systems were never intended to be connected to the corporate network or the internet. They were air-gapped, which means that security tools weren't required to protect them. However, retrofitting cybersecurity tools meant for IT networks can be challenging. On the one hand, patching is often impossible and often OT assets can't be taken offline to apply security tools. On the other hand, OT assets represent a significant investment and tend to have a lifecycle measured in decades rather than years, which means they can't be easily replaced with newer, easier-to-secure assets. And, because most IT security models are built for IT-focused attacks, they may not be able to detect or prevent attacks on the OT network.



OT is difficult to secure because these legacy systems were never intended to be connected to the corporate network or the internet.

Attacks may come from hacktivists, nation states, cybercriminals, and disgruntled insiders. Threats can include ransomware (where attackers are driven by financial profit) or sabotage (where attackers are politically or ethically motivated). Attacks can be sophisticated or unsophisticated, and the severity of the attack will depend on the experience and skill of the threat actor.

This whitepaper outlines the six key steps CI organisations can take to protect CI assets and OT.

Creating a Cybersecurity Program in Six Steps

Security programs of work can be complex, costly, and time consuming to implement. There are no quick fixes or point solutions that will solve all the issues.

Like any roadmap, the cybersecurity program should outline the organisation's current and desired future states, as well as how the organisation will achieve its objectives. This starts with identifying the CI operator's assets and assessing its security posture. Then, the organisation can develop a strategy for planning and implementing a program of work.

Buy-in from the board and C-level executives is crucial to support this program of work. The complexity involved in reaching cybersecurity maturity means significant resources will be required over a period of time. With support from the top of the organisation, these resources are more likely to be allocated and the project to succeed.

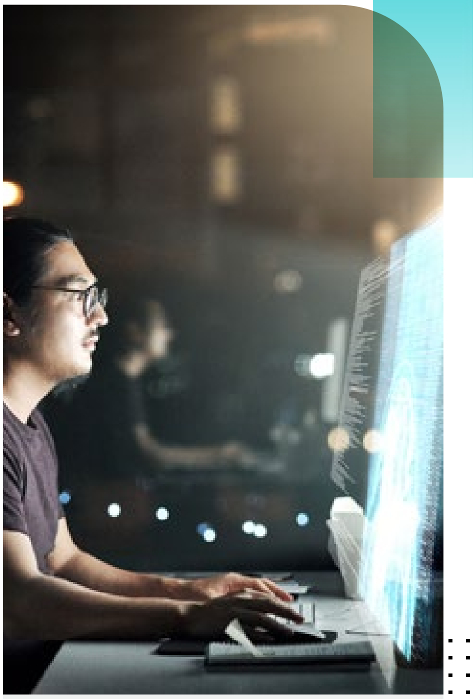
There are six key steps that CI operators will need to take to reach a secure state.

1. Risk assessment

A risk assessment is the starting place for any cybersecurity program. It's crucial to have full visibility into all assets in the OT architecture and understand what risks they may face. The risk assessment should be conducted according to a risk management standard such as ISO 31000:2019 to ensure all aspects are covered. It should define:

Terms of reference

The scope must include the domains and controls to conduct the risk assessment against, as well as the desired capability and maturity state. Examples of global standards to confirm key metrics to assess maturity against include ISO/IEC 27001:2013, NIST 800 Series, Australian Government ISM, NERC, ISA/IEC 62443, and various other industry and state-based cybersecurity models. Using these standards can help provide a structure and framework for this process, which is especially important for organisations that haven't yet reached a high level of maturity in this area.



A risk assessment is the starting place for any cybersecurity program.

A scoring system

A scoring system is key to grading the impact, likelihood, and consequence of a cyberattack. By using a capability model, organisations can determine their current capability, compare it with the risk matrix, and establish the likelihood and consequence of a cyberattack to calculate a risk score. This will let the organisation create a heat map against security domains, then score the organisation's overall security posture.

The score can then be used to help direct future efforts and resource allocation, ensuring investment is prioritised in areas where it can have maximum impact.

Industry data

The risk assessment requires access to industry data so the organisation can compare configuration settings, current version/patch release, and provide remediation recommendations.

Additional information

It's also recommended that the risk assessment team walks through the plant and other facilities to document the site managers' views on the location of assets and equipment that may generate data. During the walkthrough the risk assessment team should review:

- equipment in the server, computer room, or data centre
- RJ45 and/or RJ11 ports in walls
- modems attached to devices in racks
- asset identification and version information, using tools such as Cloroty, Nazomi, Armis, and Dragos
- which system suppliers have remote access for maintenance and monitoring
- what control systems are in place to manage remote access, including processes for granting access and whether multifactor authentication is used.

Once completed, the risk assessment results and findings should be numerically coded and transferred to the enterprise risk register to be presented at the board's risk committee meetings. Then, the IT security team can request budget for remediation activities.

The risk assessment requires access to industry data so the organisation can compare configuration settings, current version/patch release, and provide remediation recommendations.

2. Strategy and governance

Once the risk assessment is complete, the team should list the major projects that the organisation needs to complete to mitigate and/or remediate identified risks. The projects, funding, and timelines need to be mapped at this point.

At this stage, the strategy should articulate the program of work required to achieve the desired secure state so that the board can understand and sign off on the program of work. It's important to avoid overcomplication at this point so that executive boards can understand the risk in business terms.

Governance is required to ensure that projects are managed and delivered to achieve the desired outcomes on time and within budget, including structured reporting to the board for maximum confidence. Without this, the board may lose confidence in the project and become reluctant to allocate further resources to it.

3. Documentation and standards

The team needs to document the organisation's operational objectives, the assets required to meet those objectives, and the security program required to secure those assets. Security architecture documentation and an information security management system (ISMS) maps business requirements against an organisation's security program and documents requirements across people, processes, and technology to mitigate and manage risk.

It's important to use an appropriate model to create the security architecture documentation. This model could be Sherwood Applied Business Security Architecture (SABSA) or The Open Group Architecture Framework (TOGAF).

Each layer requires substantial input from internal and external resources. Once complete, the documentation will provide structure and guidance for all staff, suppliers, and contractors involved with the organisation.

Standards are also essential during this phase of the cybersecurity program. Standards have been developed over many years with the global collaboration of security experts, making them an ideal framework or checklist of things to do across multiple industries. The ISMS can be built by selecting a standard such as ISO/IEC 27001:2013, ISA/IEC 62443, NIST, or the Australian Government Information Security Manual (ISM).

The standards document should contain cybersecurity domain descriptions, processes, and controls. When implemented, organisations can track their security maturity as they continue to implement controls and processes across their architecture. The organisation can select controls described in multiple standards to develop a checklist of security objectives.

At a minimum, security documentation should confirm all the controls that need to be deployed to meet security objectives in line with business requirements. This documentation should also detail processes and procedures across multiple security domains, establish the ISMS to commence the security journey, and specify the role of management in cybersecurity decision-making.

The documentation phase is complex and comprehensive. Completing this phase successfully may take 12 months or longer depending on resources and availability. To this end, it may be valuable for organisations to work with an experienced partner to complete this phase (and others), to ensure it is accurate and comprehensive. Failing to get the documentation phase right could put the entire security program at risk.

4. Implementing and security testing

Once the risk assessment, planning and documentation are complete, it is possible to build the security architecture in its physical form.

There are usually four phases:

1. **Proof of concept:** the entire solution or key components are built and tested. This can be on site, virtually, or in a lab to prove that the conceptual architecture can deliver on business expectations and as specified by vendors.
2. **Factory acceptance testing:** the key vendors test their components individually or together as systems in their respective factories or staging areas. Once confirmed that the solution is meets operational requirements, it can be passed to the organisation for final acceptance.
3. **Site acceptance testing:** the entire solution is deployed to site and built to specification. Once installed, it is then tested to confirm it meets operational requirements, at which point the organisation can provide final sign-off.
4. **Security testing:** the end user or master contractor can use internal or independent third-party testers to conduct active or passive tests to confirm that:
    a. the security controls specified have been implemented
    b. the systems are configured correctly and are operational
    c. the key metrics are visible
    d. alerting systems are working.

Additionally, red-teaming exercises and penetration testing can identify vulnerabilities and report them for remediation.

The documentation phase is complex and comprehensive. Completing this phase successfully may take 12 months or longer depending on resources and availability.

5. Monitoring, threat intelligence, and incident response

Once the security architecture is in place, it's essential to ensure ongoing visibility across the architecture and that the security team is alerted to operational and security events based on a series of rules. The monitoring phase requires strong planning to achieve appropriate outcomes.

Metrics should be collected across four key areas:

1. **Operational performance**, to confirm whether assets are performing as expected.
2. **Application performance**, to confirm whether applications are performing as expected.
3. **Security**, to understand correlation rules, what certain indicators mean, and the external threat feed.
4. **Business**, to ensure the systems are delivering the desired outcomes.

Operations teams need to collect log data from across the architecture to report on performance according to specified requirements. The baseline data may be collected via machine learning or artificial intelligence. The data can then be used to define normal operations versus alerts to be reported, and, to notify key personnel of unexpected activity that should be investigated.

Organisations can get a more detailed picture of the security posture by combining security data with threat intelligence. Application data can be captured in line with specified metrics to confirm applications are also performing as expected.

Overall, this can provide businesses with insight into the risks they face, the vulnerabilities that are present in their architecture, and how security controls may need to be adjusted to improve protection.

When security incidents occur, incident responders will require access to logs and operating data to identify and manage those incidents effectively. Without this information, it is impossible to set a reference point for normal activity and define and detect cyber incidents.

The final part of this phase is to create an incident response plan. Incident response includes preparation, detection and analysis, containment and recovery, and post-incident activity. The response plan can be socialised internally to ensure everyone in the organisation, from the CEO and CIO to marketing and forensic investigators, clearly understands their role in the incident response process.

Organisations can get a more detailed picture of the security posture by combining security data with threat intelligence.

6. Training

The most effective cybersecurity measures will be rendered useless if the organisation doesn't have a strong cybersecurity culture. Training must be part of induction programs and delivered regularly for general staff. In-depth courses are required for IT and OT staff.

The most effective types of training are:

1. **Cybersecurity awareness:** ongoing training including basic security concepts, major threat types and sources, methods of breach and simple countermeasures, human firewalls, and what constitutes a security culture.
2. **Documentation:** training on the people, process, and technology documentation, which is usually conducting during onboarding.

The Way Forward

The threat landscape continues to evolve and CI operators will remain at risk of serious cybersecurity attacks. It's essential to act now to begin the lengthy and complex process of implementing a strong security posture.

These six key steps are essential for organisations seeking to reach a secure state. Skipping even one step will compromise the organisation's ability to reach cybersecurity maturity. This requires a commitment from the board and executives, as it will consume resources and time. Cyberattacks on CI operators are likely to increase and the potential effects can be catastrophic. Organisations should act now and start their journey towards cybersecurity maturity.

Establishing a program of work that addresses each of the six key steps outlined will help organisations protect their CI assets and comply with the *Critical Infrastructure Act*.

Fortinet's security fabric approach integrates a broad set of automated solutions that work together to deliver state-of-the-art security operations. Together, these solutions create a comprehensive, reliable, and cost-effective approach to protect the entire organisation, including OT systems. By adding a security fabric strategy, CI operators can lower the risk of undetected security vulnerabilities and leverage the power of automated solutions to achieve a more secure state.

[1] David Pearce, et al., "Changes to Critical Infrastructure Laws in 2021: Is Your Sector Impacted," MinterEllison, February 17, 2021.