Cyber Security in Mining, Energy, Construction and Supply Chain

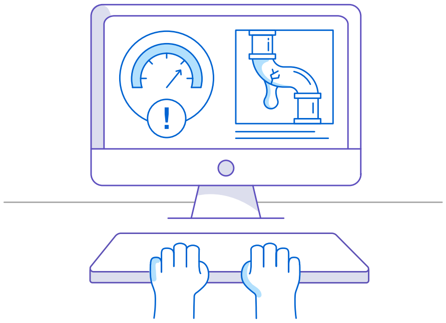
Cybersecurity poses distinct challenges for the mining, energy, construction and supply chain industries, and they are further compounded by the convergence of OT and IT network infrastructure, software tools and management policies.

In the past, cybersecurity has been the domain of IT

Over the past few years, there has been a consistent increase in malicious cyberattacks aimed at Australian organisations. According to the latest statistics from the Office of the Australian Information Commissioner (OAIC), there were 497 notifiable data breaches reported between July and December 2022, a 26 percent increase on the first half of the year. The report noted that 350 breaches were the result of 'malicious or criminal attacks', a rise of 41 percent over the previous half.[1]

Threats have included unauthorised or compromised system access, data loss or theft, intentional or accidental introduction of a virus, unauthorised money transfers or payments, suspicious network activity, unauthorised hardware, and ransomware.

Now consider Operational Technology (OT)



Modern factories, mining/construction sites and utilities suppliers with critical infrastructure assets, rely on Operational Technology (OT) to improve the efficiency and management of their industrial machinery. This can include manufacturing, order/despatch, supply chain and any number of industrial control systems (ICS). Regardless, the purpose is to ensure these systems are operating at maximum capacity with minimum downtime.

Any changes to these environments are realised immediately and have real world (physical) consequences.

For decades, OT systems have operated at arm's length from IT environments. While connected to a network, they were rarely coupled with IT networks and the Internet.

The convergence of IT and OT

Today's organisations expect more from their OT. They expect these devices to be connected. That policies and procedures are normalised across OT and IT network infrastructure. A simple example of convergence in action: smart sensors, which provide granular analytics for maintenance and drive efficiency across remote and fixed machines. The smart sensors are sometimes considered OT, yet the data gathered can be via IT applications.

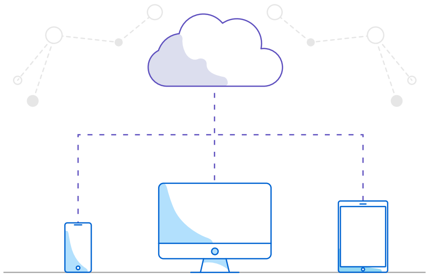
Another aspect is Internet of Things (IoT). IoT allows organisations to use collected data across remote devices to help monitor, maintain, optimise and drive efficiency and productivity across the organisation. There is growing recognition amongst industry leaders regarding the power of insights from data analysis and how it can drive real time decisions, enhance predictive modelling and improve safety.

Both IoT and convergence, more generally, have implications for cybersecurity.

[1] 'Notifiable Data Breaches Report, July-December 2022', Office of the Australian Information Commissioner, March 2023

What is Operational Technology (OT) security?

Traditional OT assets can be difficult to secure due to their design for maximum availability and safety coupled with their use of decades-old systems that often lack recent security updates. Because updating OT can be both difficult and expensive, the mindset has traditionally been to leave as is, until a problem presents itself.



As OT environments are becoming increasingly connected to other networks, their devices, their applications and cloud services that facilitate their remote control and operations are vulnerable to increased cyber risk.

Mining, Energy, Construction and Supply Chain Challenges

Securing traditional Operational Technologies/Industrial Control Systems (OT/ICS) assets has proven challenging due to:

Siloed IT and OT systems

One of the most significant inhibitors to industrial automation, often with differing policies and procedures across IT and OT.

Legacy technology

The challenge of aged OT assets is not uncommon, with operational cycles of up to 25 years.[2]

The data-driven imperative

Executives cited creating a data-driven organisation as one of their top 10 priorities (86% in mining/utilities, 81% in manufacturing and 66% in construction). However, the focus of OT has been on high availability and safety, less about insights and the necessary security updates.[3]

Budget and skills

Many organisations are challenged with a limited budget to update their OT assets. Most require consultative technology partners with expertise across networks, connectivity, cloud, security and IoT to bring the full value of convergence to the organisation.

[2] Telstra Market Book – Mining, Energy and Construction & ASCR, 2022

[3] ADAPT Research – Business Priorities by Industry, 2022

Why Telstra for OT Security

In 2022, Telstra Purple acquired **Alliance Automation**, one of Australia's largest independent providers of **industrial automation solutions and control systems.**

Founded in 2010, Alliance Automation is staffed by more than 250 engineers and consultants. It provides services in **technical advisory and design, electrical and automation engineering, project management, site installation, business intelligence, operational technology cyber security and 24x7 support.**

Alliance Automation specialises in delivering **value added solutions, consultancy and support to customers** in mining, utilities, infrastructure, construction, manufacturing and supply chain markets both in Australia and overseas.

It is the full ecosystem - Telstra, Telstra Purple, Aqura and Alliance Automation – that can now deliver customers a comprehensive solution, starting with **connectivity and professional and managed services capabilities** while expanding the potential for **digital transformation services, industrial automation capabilities, digital twins, smart spaces and operational technology cyber security.**

For case studies, visit: https://allianceautomation.com.au/projects/

Now Available: IT/OT Security Risk Assessments

Alliance Automation and Telstra Purple now provide IT/OT Security Risk Assessments, which are accessible to specific customers in the mining, energy, construction and supply chain sectors. Based on your needs, this may include an:

OT Audit	Conducting a comprehensive inventory assessment of all OT infrastructure, including PLCs, servers, network switches, gateways, and firewalls.
Asset vulnerability discovery exercise	Gathering and analysing the traffic between OT devices to detect potential vulnerabilities.
OT security assessment	Identification of security gaps and missing controls to gauge the maturity level of the organisation's approach to OT cybersecurity. Using this information, our team can provide suggestions for achieving target maturity levels and constructing strategic deployment roadmaps.
OT third-party risk assessment	Working with essential third-party stakeholders, like Original Equipment Manufacturers (OEMs) or service providers, to evaluate the current security measures in place and identify any gaps in OT security across the supply chain.
OT governance framework	Helping define the OT cybersecurity strategy, create a functional IT/ OT governance working model and alignment with the organisational Governance Risk and Compliance (GRC) framework to support OT business case development.
Cyber Security Essentials Assessment	This assessment provides a comprehensive understanding of your organisation's existing IT security posture, both on-premises and in the cloud. Responses will be analysed against standards and frameworks from ACSC (Essential 8 and Top 37), APRA (CPS234), International Standards Organisation (ISO27001), the Cloud Security Alliance (CCM4), and the US National Institute for Science and Technology (NIST CSF).

For more information visit:

www.telstra.com.au/industrial-automation