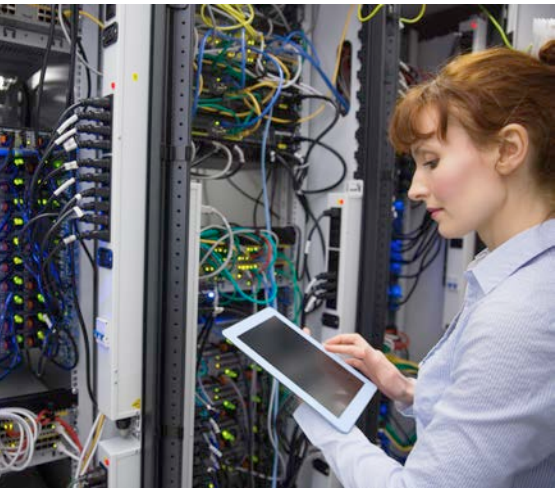
10 most likely ways your operational technology network will be compromised
December 2015

Cyber savvy: Securing operational technology assets



pwc

www.pwc.com.au

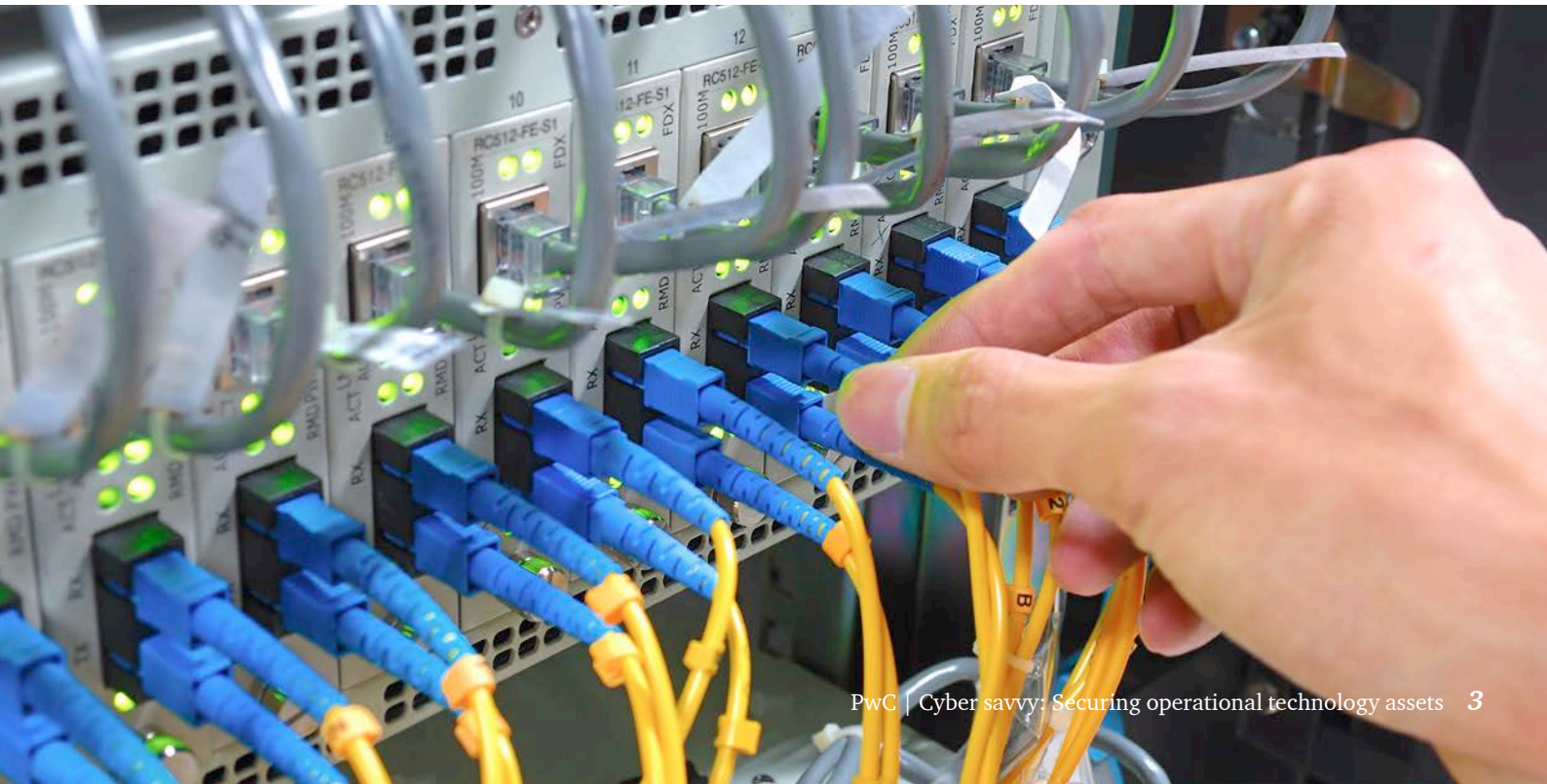
Contents

Cyber savvy: Securing operational technology assets

Business leaders who have security as part of their overall business strategy discussion are better positioned to balance the technologies, processes and resources needed to anticipate constantly evolving cyber risks. But in the energy, mining and utilities (EM&U) sectors, the focus should not just be on corporate IT systems as there are just as significant security threats to operational technology.

The term 'operational technology' (OT) refers to the hardware and software used to control industrial processes. A cyber attack on an OT environment can have serious and wide ranging consequences beyond just financial losses – including prolonged outages of critical services, environmental damage and even the loss of human life. There are highly skilled and motivated adversaries actively seeking to exploit the security weaknesses in OT networks, process control systems and critical infrastructure. Their motivations range from economic benefit and espionage through to malicious disruption and destruction.

While many operators in these sectors have recognised the need to increase focus and spending on the security of their corporate IT systems, this has not been matched for OT systems, leading to critical vulnerabilities.



We have drawn on our experience conducting cyber security assessments and penetration tests from across our global network to identify the 10 most common security vulnerabilities in OT networks:

"As a society, we all depend on operational technology for a wide range of critical industrial processes. The continued and regular sharing of cyber security intelligence and insights is essential to improving the resiliency of these systems and processes from emerging cyber risks."

David Gracey, Chief Information Security Officer, Rio Tinto

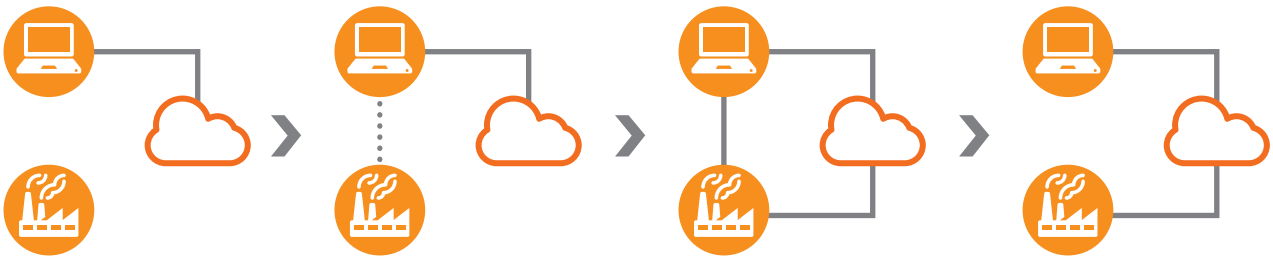
- Publicly accessible OT systems
- Insecure remote connectivity to OT networks
- Missing security updates
- Poor password practices
- Insecure firewall configuration and management
- OT systems located within corporate IT networks
- Weak protection of the corporate IT network from OT systems
- Lack of segmentation within OT networks
- Unrestricted outbound internet access from OT networks
- Insecure encryption and authentication for wireless OT networks.

By identifying cyber security flaws and the risks these vulnerabilities present, decision-makers will be better placed to implement appropriate security controls, design more secure architectures, monitor targeted attacks and maintain effective cyber resilience for their OT networks.

The price of interconnectivity

OT systems have long been used in manufacturing, mining, energy, utilities, logistics and other industrial operations to monitor and control physical processes. Traditionally, these technologies have been 'air-gapped' whereby they are segregated from the organisation's corporate IT network. However, as the following diagram shows, OT systems are becoming increasingly interconnected and integrated with other IT systems.

Economic challenges, resource constraints, business requirements and technology standardisation have made it impractical to continue completely segregating OT networks from IT networks. Cyber attacks on IT networks occur regularly, and so the trend towards increased integration means that OT devices may be reached and ultimately compromised through IT networks. This widens the attack surface as vulnerabilities in IT networks can be used to mount attacks on OT networks.



1980s

- IT and OT operate in different environments and on different platforms
- OT are based on proprietary platforms
- Data is not shared between technologies

1990s

- OT is networked to allow centralised operation

2000s

- OT connects to IT using standardised IT channels to reduce costs and increase compatibility
- Boundaries between IT and OT start to blur

2010+

- The technology underlying IT has become ubiquitous across OT
- The combination represents the integrated technology ecosystem

Information technology (IT)

Operational technology (OT)

Internet

Proprietary connection

IT protocol-based connection

Top 10 OT network vulnerabilities

1. Publicly accessible OT systems

OT systems are often directly connected to the internet, in some cases so that third-party vendors can remotely connect to the system to perform diagnostics and maintenance. In many of these instances, the OT systems are not protected by a firewall and are outdated, so they lack modern security features that would typically be used to protect an internet-facing connection (e.g. multi-factor authentication, strong passwords, logging and monitoring).

This issue means that potential attackers can directly perform password 'brute-forcing' (a method of rapidly attempting different potential passwords) or probe these interfaces, which can cause OT systems to become unstable or fail completely, resulting in business disruption.

If remote support is required, an enterprise-grade firewall, a remote access solution and multi-factor authentication should be implemented to control all access to OT devices and systems.

2. Insecure remote connectivity to OT networks

A 'jump box' is a remote connection system that gives an operator access to the OT network from the corporate network. The jump box often serves as the single point of entry to the OT network. These jump boxes are remotely accessible and may provide significant access to the OT network; as such they are an attractive target for attackers.

Common vulnerabilities that are seen elsewhere also apply to jump boxes. Attackers only require any one of these vulnerabilities to be present in order to gain access to OT systems.

The use of a strong, multifactor authentication mechanism, enforced password policies and appropriate security patching practices can minimise the risk of compromise through these attack vectors.

3. Missing security updates

Availability is a key requirement in an OT environment, and unplanned downtime can have significant consequences. This can lead to a conservative approach to deploying software patches and updates, as these new patches can have unintended consequences.

The inherent danger of this approach is that OT systems end up running outdated software versions with known security vulnerabilities, leading to increased risk of compromise by an attacker.

Processes and procedures should be established to thoroughly test patches and updates to OT systems. Given the potential to disrupt operations, patches and updates should be installed on a representative sample of systems before going live to production systems. This may be an isolated test environment with identical systems, or, if testing in a live environment, it should be possible to failover to redundant devices that have yet to be updated.

If a patch is found to cause production issues, other complementary controls such as segregation, authenticated access, logging and monitoring, firewall and device hardening may be employed to reduce the probability of compromise.

4. Poor password practices

Even those businesses that have strong corporate password standards often fail to apply these to their OT environment. Common issues include:

- operators and administrators using the same usernames and passwords for corporate and OT systems, enabling attackers to easily pivot from the corporate network into the OT network
- generic user accounts usually having easily guessable passwords or passwords that are identical to the user name. These accounts are used on multiple systems allowing an attacker to propagate through the OT network
- failure to change default vendor credentials on embedded devices and management interfaces from the initial installation or setup. The use of default credentials is one of the most common ways attackers gain entry into a system.

Organisations need to establish and maintain a strict separation between authentication mechanisms and should require separate username conventions for the corporate IT and OT networks. They must also develop a process to change default credentials from software and devices during initial configuration. Compliance with secure password policies for both IT and OT networks should be enforced through controls such as security audits.

5. Insecure firewall configuration and management

Firewalls that segregate OT networks from corporate networks are an essential control in protecting both networks. However, insecure configuration and management of these firewalls significantly increases the potential attack surface of the OT network. Common vulnerabilities include misconfigured access rules allowing unnecessary access between corporate IT and OT networks, and temporary rules that have outlived their purpose. It is also common for support teams to allow excessive access to management interfaces on firewalls.

Without properly secured firewalls, security threats to the corporate IT network can easily propagate to the OT network, leaving it susceptible to attack.

A secure firewall configuration and a formal firewall change management program will help to protect OT networks from perimeter attacks originating from the corporate or external network. It is critical to restrict access based on business need, and to perform regular audits of all connections between IT and OT networks.

6. OT systems located within corporate IT networks

Corporate systems usually require some level of interconnectivity with the OT network in order to access operational data or export data to third-party management systems. OT components such as reporting servers and control stations are frequently placed within the corporate network, connecting through to the OT network, instead of being constrained to the OT network.

The increasing frequency of cyber attacks on corporate IT networks means this type of 'overlap' between the networks poses a serious risk as attackers may be able to use a compromised corporate IT system to then access OT networks.

A strong segregation between corporate IT and OT devices provides a layer of defence to protect OT devices from external cyber attacks. Where there is a business reason for the two systems to overlap, a demilitarised zone (DMZ) should be established for all connections between the two networks. It is also advisable to regularly monitor all DMZ activity between the IT and OT networks.

7. Weak protection of the corporate IT network from OT systems

While companies are increasing their focus on mitigating OT network attacks that originate in the corporate IT network, there is a general neglect for attacks originating from the opposite direction (i.e. from OT devices to the corporate IT network). OT systems often use legacy technology, spread over disparate and remote locations. Additionally, the physical security measures for remote stations and field devices can be weak.

Connectivity to the corporate IT network, from the OT network, may provide a pivot to gain entry into the corporate environment through insecure OT devices, increasing the risk of unauthorised access.

It is important to restrict access between these two networks, based strictly on business need. Any connection between the OT network and the corporate IT network should be through systems hosted in a DMZ, or secure gateway between the two networks. Organisations should also avoid hosting corporate systems within OT networks, with any exemptions requiring a formal risk assessment.

8. Lack of segmentation within OT networks

Many OT networks are designed and configured in a flat and unsegmented configuration to simplify management of the network.

Unfortunately, this flat layout increases risk by assuming all systems are of equal importance, function and criticality. A breach of any single device may expose the entire OT network.

Defining a clear separation between critical and non-critical systems not only limits the impact of a breach, it also helps to clarify the organisation's OT 'crown jewels' and apply appropriate security controls. Implementing a zoning model that uses a 'defence in depth' approach makes it harder to impact the OT network or services as an attacker must penetrate several layers of defence to compromise critical systems.

9. Unrestricted outbound internet access from OT networks

In some instances, direct outbound internet access is enabled from the OT network, usually to allow for patching or for operator maintenance research.

As discussed previously, OT systems commonly run outdated software, so enabling direct outbound internet access significantly increases the risk of malware being introduced to the OT network. Unpatched and insecure OT hosts are particularly susceptible to infection by malware and propagation throughout the broader network.

Direct internet access from the OT network also increases the risk of external command-and-control attacks, whereby an attacker establishes reverse connections to 'phone home' and issue real-time commands to the compromised OT systems.

Outbound access to the internet from OT systems should be restricted, with any exemptions requiring a formal risk assessment. In the case of such exemptions, OT systems requiring external access must be securely patched, closely monitored and appropriately segregated from the rest of the OT network. Security updates can be downloaded from the internet onto a separate repository outside the OT network and verified in a test environment before they are ported onto OT systems.

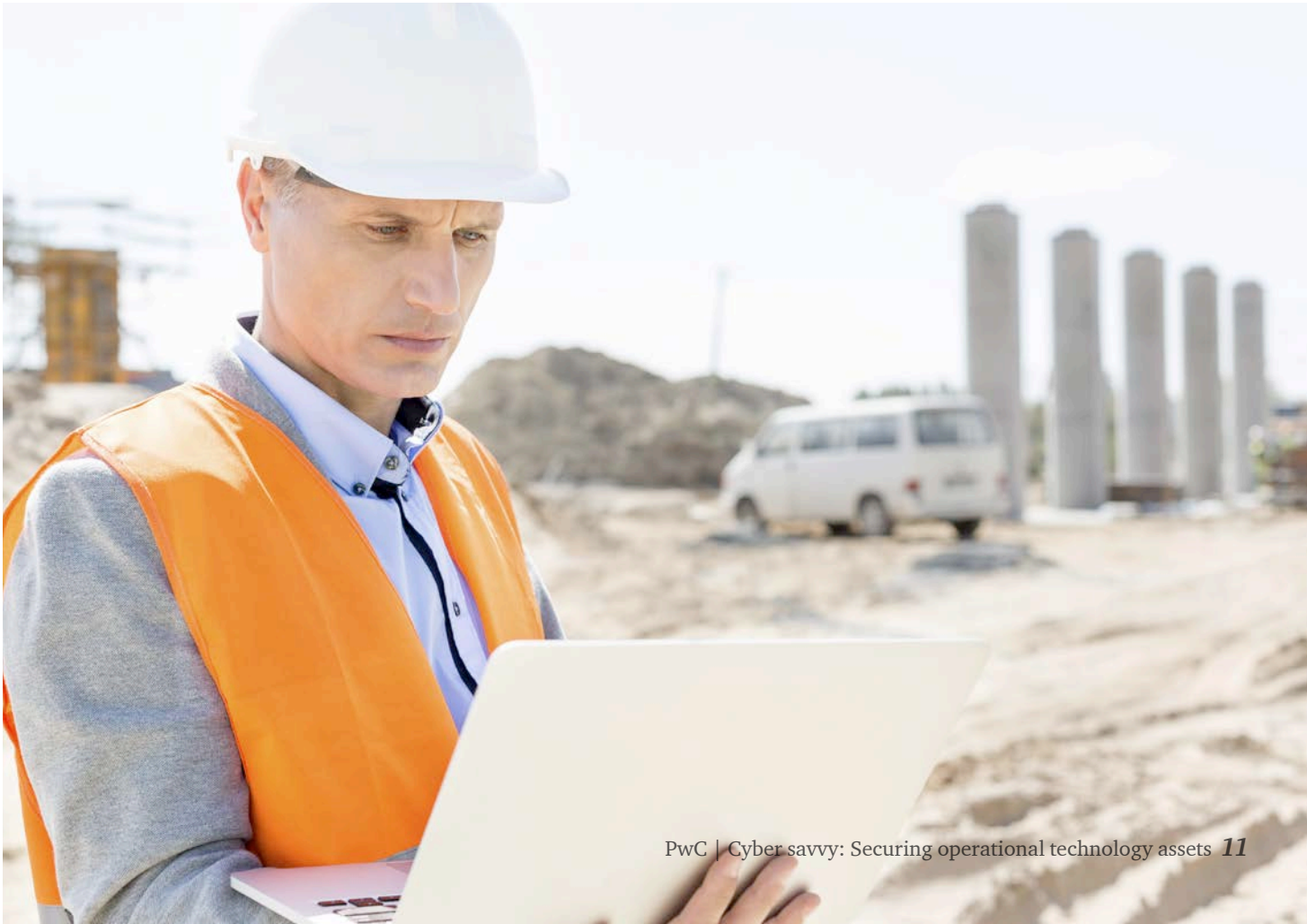
10. Insecure encryption and authentication for wireless OT networks

OT networks often use wireless and microwave solutions to connect devices and systems, sometimes over considerable distances. In some instances, radio telemetry technologies such as WiMAX and LTE are used to connect remote stations and field devices when physical communication channels are not available.

It is not uncommon for the deployed wireless equipment in OT networks to use deprecated security protocols or technologies, leaving them vulnerable to modern eavesdropping and authentication bypass attacks. An attacker in close proximity may be able to gain direct access to the OT network, allowing them to launch further attacks within the broader network.

The cost of radio equipment required to launch malicious attacks against wireless networks, including proprietary wireless protocols, has dropped significantly in the last five years, making such attacks easier and cheaper to execute.

Using strong wireless encryption protocols, industry-standard cryptographic algorithms and mutual authentication between communicating OT systems is the best way to minimise the risk of wireless attacks. Any outdated or deprecated communication solutions should be refreshed, and wireless systems should be audited on a regular basis.



How to mitigate against a successful OT network cyber attack

A successful exploitation of any one of these 10 common security vulnerabilities could be far reaching, including losses in production or revenue, damage to the environment, regulatory fines, reputational damage and even catastrophic shutdown of national infrastructure and loss of life. Businesses with OT networks need to be in a position to assess, identify and rectify cyber security vulnerabilities if they are to prevent malicious attacks that exploit these vulnerabilities.

Security strategy and executive support

Maintaining a secure and resilient OT environment requires a comprehensive strategy that covers security governance and process, implementation of the right technology and employing people with the right skills. The strategy needs to have support at the executive level, and be clearly communicated to all stakeholders. A lack of understanding of cyber risks and inadequate cooperation between the relevant business, IT and OT teams is often a significant factor in network security breaches.

An information security awareness program is critical to protecting OT networks and assets, and organisations within the EM&U sector can often best achieve this by leveraging their already strong safety cultures to promote a message of 'cyber safety'.

The right cyber skills

Relevant and adequate skills are another key element to maintaining secure OT networks. Skilled information security professionals understand the unique challenges facing operational networks and are able to identify and communicate shortcomings in network implementation, architecture designs, technology configuration and business impact analyses.

There are certain types of assessments that will require specialist cyber security skills, such as penetration testing of OT environments, in order to minimise potential adverse impacts to the business. Having the right people in place will enable the organisation to prevent, mitigate, respond and resolve cyber security incidents as they arise.

Relevant, properly configured technology

Investment in the right technology is another key characteristic of a resilient OT network. A strong collaboration between well-equipped IT and OT teams is also necessary for a unified approach to risk management and incident response. Using the right detection, prevention, monitoring and reporting tools helps organisations to prevent attacks and facilitate informed decision-making in relation to possible cyber security threats.

Where to from here?

Organisations in the EM&U sectors are particularly reliant on OT networks to control their critical industrial operations and infrastructure. Our work on global engagements identifies that many of these OT networks are susceptible to cyber attacks with potentially catastrophic consequences, including significant environmental damage and even the loss of human life. By identifying the 10 most common security vulnerabilities we have encountered, we are hoping to raise awareness of the risks and, in doing so, help EM&U sector operators address these vulnerabilities.

Businesses can create more resilient OT networks through the effective use of skilled resources and suitable technology, including the integration of defence in depth techniques across IT and OT networks. The National Institute of Standards and Technology (NIST) has produced a guide for Industrial Control Systems (ICS) Security (SP 800-82) which explains best practice for businesses to design security into their OT environments. Business leaders also need to ensure there is an organisationwide awareness of the cyber security risks that exist, and enforce the strict mplementation of security policies to address these vulnerabilities.

Contacts

Contact the following EU&M cyber security leads for further discussion on how we can help your organisation address the security challenges in your OT environment:

Mike Younger

Partner
+61 490 093 981

mike.younger@au.pwc.com

Andrew Gordon

Partner
+61 402 892 184

andrew.n.gordon@au.pwc.com

Robert Di Pietro

Partner
+61 418 533 346

robert.di.pietro@au.pwc.com

Duncan Alderson

Managing Director
+61 481 000 858

duncan.alderson@au.pwc.com

127034125