OPERATIONAL TECHNOLOGY CYBERSECURITY

A guidance on helping clients secure their OT environments and industries

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

CONTENTS

A word from Jean-Marc Imbert 3

Are you failing to ensure that your Operational technology environment is resilient? 4

The Security of Critical Infrastructure Act 2018 (SOCI Act) 7

The Bills as a framework 7

Who does the bill apply to? 8

How can RSM help you protect your critical OT environment? 10

A WORD FROM JEAN-MARC IMBERT

Welcome to the RSM's industry note and guidance paper on OT Cybersecurity

The industrial control system (ICS)/operational technology (OT) security community is witnessing risks that go beyond traditional attacks on enterprise networks.IT security is no longer the black box it used to be.

However, OT security remains an area that is not covered well enough. Cyber-attacks are increasingly traversing from Information Technology (IT) to OT environment creating real-world critical impact on operations, health and human safety.

OT underpins a lot of the critical infrastructure we see within Australia. An attack on an OT environment by an adversary can impact our way of life and endanger human safety. As a result, OT security is a critical area of focus. The Security of Critical Infrastructure (SOCI) bill that was passed in its full form earlier this year reiterates the required focus in this space.

Considering this and our wider experience supporting cybersecurity needs of organisations worldwide, RSM is committed to helping clients secure their OT environments and industries within Australia more broadly.

Our approach and our capability are documented within this paper.

If you require any further details on any of the articles in this edition, please contact your local RSM representative or drop me a line.

On behalf of the team at RSM we look forward to partnering with you on your OT resilience journey.

Jean-Marc Imbert
National Head of Risk Advisory
jean-marc.imbert@rsm.com.au

Are you failing to ensure that your Operational technology environment is resilient?

Cyber security incidents are continuing to grow exponentially globally. OT environments differentiate themselves from the IT environments in terms of their business purpose and have traditionally not been as well secured. Unfortunately, cyber criminals have also realised this and are now ramping up attacks on critical infrastructure.

Operational Technology (OT) is key to automating and driving efficiencies within multiple sectors including manufacturing, mining, utilities, etc. However, if this OT is not adequately secured, it makes the entire environment vulnerable to cyber-attacks.

OT environments can be seen as a soft underbelly because they have not had the cyber security attention like their IT cousins have had. We are now confronted with an ever- increasing dilemma that IT and OT environments are converging leading to security vulnerabilities traversing from one to the other. OT devices are proliferating which naturally increases the attack surface. Furthermore, OT devices have not always been designed with cyber security in mind or run by cyber security professionals, thus making them even more vulnerable.

Since OT devices control production systems, any outages can be devastating.

A huge focus – rightly so – is placed on ensuring the operational technology is running constantly, but a sole concentration on keeping the lights on leaves vulnerabilities, which hackers can and have exploited. This relative immaturity of cyber security for OT environments represents a challenge, but also an opportunity. It is not too difficult to secure OT environments if we just focus on the basics. This is where the IEC 62443 standard comes into play.

OT environments traditionally have not been as well secured as IT environments and this paper aims to summarise the basic controls that should be in place within OT environments to harden them against cyber-attacks.

What do you need to do?

To secure OT environments against the modern-day cyber-attacks, we must cover the following basics:

- **Visibility** – This is the most important control. Without this control, there is no point trying to implement any of the controls noted below. Document your OT environment. Cover the devices, the connections, architecture, network configuration, security configuration, etc. Update this information monthly as OT devices tend to proliferate. Without knowing what you have, you cannot secure it.

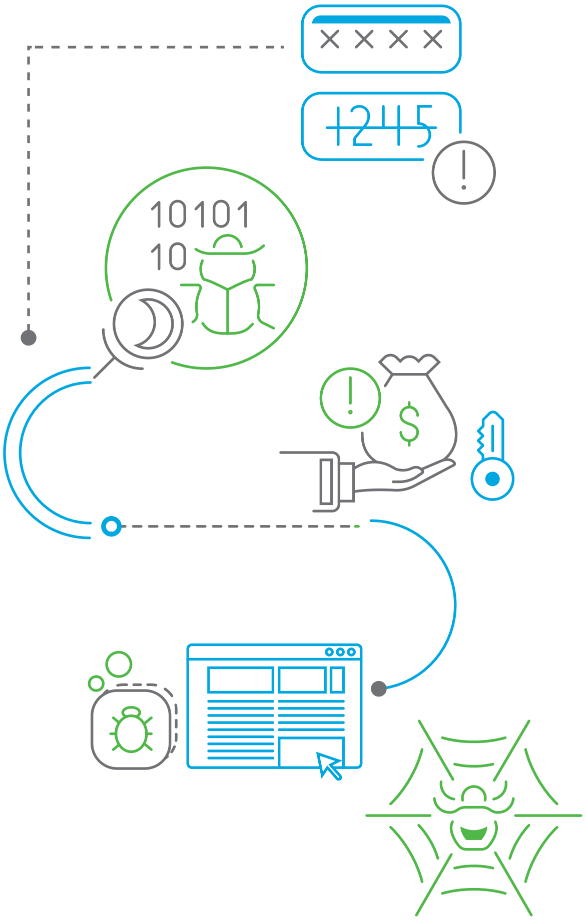
- **Segregate and cloak OT networks** – Ensure you are running OT networks that are separated from other networks. Macro-segmentation from IT networks is not enough. It is important to microsegment the OT network into functional zones based on criticality to protect zones from each other and prevent any cyber-attacks traversing zones. It is also important to cloak each zone from each other to prevent discovery of devices from other zones and stop attackers or malware/ ransomware from traversing zones.

- **Remote access security** – Due to the function that OT devices serve, remote access and management is a necessity. This access must be secured. An ideal way to provide this is to use the concept of Zero Trust Network Access (ZTNA). This dictates point-to-point secure access over an encrypted channel that is restricted to a set of source and destination devices only. This access must be governed using multi factor authentication, authorisation and adequate logging and alerting controls.

- **Device hardening** – Ensure you understand all the security features available with OT devices and configure them appropriately. This is necessary to ensure that OT devices can withstand cyber-attacks. For legacy devices that cannot be secured adequately, cloaking is a critical mitigating control that will 'hide' the devices from an attacker or malware.

- **Patching** – It is vital to keep all OT devices patched up to the right patch levels. Patches help protect against security vulnerabilities and without these patches in place, OT devices will remain vulnerable. Again, for legacy devices that cannot be patched easily, cloaking is a valid mitigating control.

- **Security monitoring** – Similar to IT networks, OT networks should also be monitored for security events. Monitoring unusual behaviour or unusual network traffic can be a good indicator of compromise that should be acted on in a timely manner. Where possible, an automated response system that can isolate the affected OT device should be used. However, depending on the device's function, this may not be desirable.



- **Basic authentication, authorisation, account and lockouts controls** – Similar to IT systems, OT systems should have authentication, authorisation, user account, password and lockout controls. These should be configured appropriately and in line with policy to harden the devices and reduce the risk of a successful cyber-attack. These controls should apply to applications, devices and users in line with the principles of Zero Trust. This should be extended to include identity-based microsegmentation to allow segmentation and access strictly based on roles defined for applications, devices and users. The microsegmentation technology should support standard PKI and certificate-based authentication to enhance the integrity of the authentication process.

- **Implement intrusion detection, malware detection, vulnerability management, hybrid threat detection (IDS, YARA Malware Detection, Threat Intelligence Feed) and Dashboard/Reporting** – These set of controls will go a long way to helping detecting threats within your OT environment and will allow you to respond to potential intrusions in a timely manner.

> As OT environments proliferate in the healthcare sector, so do the attacks. OT environments are a key target for adversaries as they are linked to production environments, the availability of which are key to several critical functions

- **Wireless network access controls** – wireless devices and users should be authenticated and controlled to protect the wired network from wireless attacks. It is advisable that wireless networks are microsegmented from wired networks. Wireless networks should have adequate intrusion detection and rouge device detection controls implemented. The latter should be enhanced with an automated response that isolates unauthorised wireless devices upon detection.

- **Protecting the integrity of data transmissions** – where feasible, all data transmitted within the OT network should be encrypted. This will not only protect the integrity of the transmitted data but will also provide an adequate control against man in the middle attacks.

- **Prohibit unnecessary functions, ports, protocols, and services on OT devices** – This will greatly reduce the attack surface of these devices and harden them against cyber-attacks. For devices where this level of hardening cannot be performed, that should be cloaked to 'hide' them from potential attackers.

- **Backup all critical data and configurations** – It is important to backup all critical data and configurations so you can perform a timely recovery from a disaster. Ensure that backup systems are segregated from production systems to prevent cyber-attacks traversing production systems and into back-up systems.

- **People and process** – Personnel must be security trained specifically for OT environments. They must understand basic security concepts and controls that have to be implemented within the OT environment that they will be managing.

> **Security policies for OT environments must be developed that outline the controls that need to be implemented and typically emphasise required areas. Without these, OT security will likely be ad –hoc and exposed to numerous vulnerabilities.**

Ashwin Pal
Director, Cyber Security and Privacy Services

The Security of Critical Infrastructure Act 2018 (SOCI Act)

No one will argue that the cyber threat landscape is changing rapidly for the worse. We have seen an increasing number of attacks on critical infrastructure lately. Motivations for these attacks vary from financial gain to nation state attacks with the aim of causing damage and destruction to another nation.

The Australian government has responded to this new threat by proposing the Security Legislation Amendment (Critical Infrastructure) Bill 2020 to bolster the Security of Critical Infrastructure Act 2018 (SOCI Act).

The Bill has subsequently been split into two now. Bill One is designed to deal with immediate threats which has now been passed into law. Bill Two is designed to deal with what are deemed the less urgent elements.

The Bills as a framework

The Bills introduce the following key concepts:

BILL ONE

- Requiring notification of cyber security incidents
- Requiring certain entities relating to a critical infrastructure asset to provide information in relation to the asset, and to notify if certain events occur in relation to the asset
- Setting up a regime for the Commonwealth to **respond** to serious cyber security incidents

BILL TWO

- The keeping of a register of information in relation to critical infrastructure assets
- Requiring the responsible entity for one or more **critical infrastructure assets** to have, and comply with a critical infrastructure risk management program
- Imposing enhanced cyber security obligations that relate to **systems of national significance**
- Allowing the minister to require certain entities relating to a critical infrastructure asset to do, or refrain from doing, an act or thing if the minister is satisfied that there is a risk of an act or omission that would be prejudicial to security
- Allowing the Secretary to require certain entities relating to a critical infrastructure asset to provide certain information elements
- Allowing the secretary to undertake an assessment of a critical infrastructure asset to determine if there is a risk to national security relating to the asset

The applicability of the above is best summarised below:

	Entities within Critical Infrastructure Sectors	Critical Infrastructure Assets	Systems of National Significance
Government Assistance	Yes	Yes	Yes
Positive Security Obligations	No	Yes	Yes
Enhanced Cyber Security Obligations	No	No	Yes

Who does the bill apply to?

Per Bill One, this applies to the following sectors. Please note that the bill outlines the definition of each sector as well as its Critical infrastructure assets:

- Communications sector
- Data storage or processing sector
- Financial services and markets sector
- Water and sewerage sector
- Energy sector
- Health care and medical sector
- Higher education and research sector
- Food and grocery sector
- Transport sector
- Space technology sector
- Defence industry sector

RISK MANAGEMENT PER BILL TWO

Risk management related to critical assets forms the backbone of this Bill. The SOCI Act and the proposed changes will ultimately require responsible entities of critical infrastructure assets to manage security risks by meeting the following **principles-based outcomes**:

- **Identify material risks** – Entities will have a responsibility to take an all-hazards approach when identifying risks that may affect the availability, integrity, reliability, and confidentiality of their asset
- **Mitigate risks to prevent incidents** – Entities will be required to understand the identified risks and have appropriate risk mitigations in place to manage those risks
- **Minimise the impact of realised incidents** – Entities will be required to have robust procedures in place to mitigate the impacts in the event a threat has been realised and recover as quickly as possible
- **Effective governance** – Through rules, entities will be required to have appropriate risk management oversight arrangements in place, including evaluation and testing

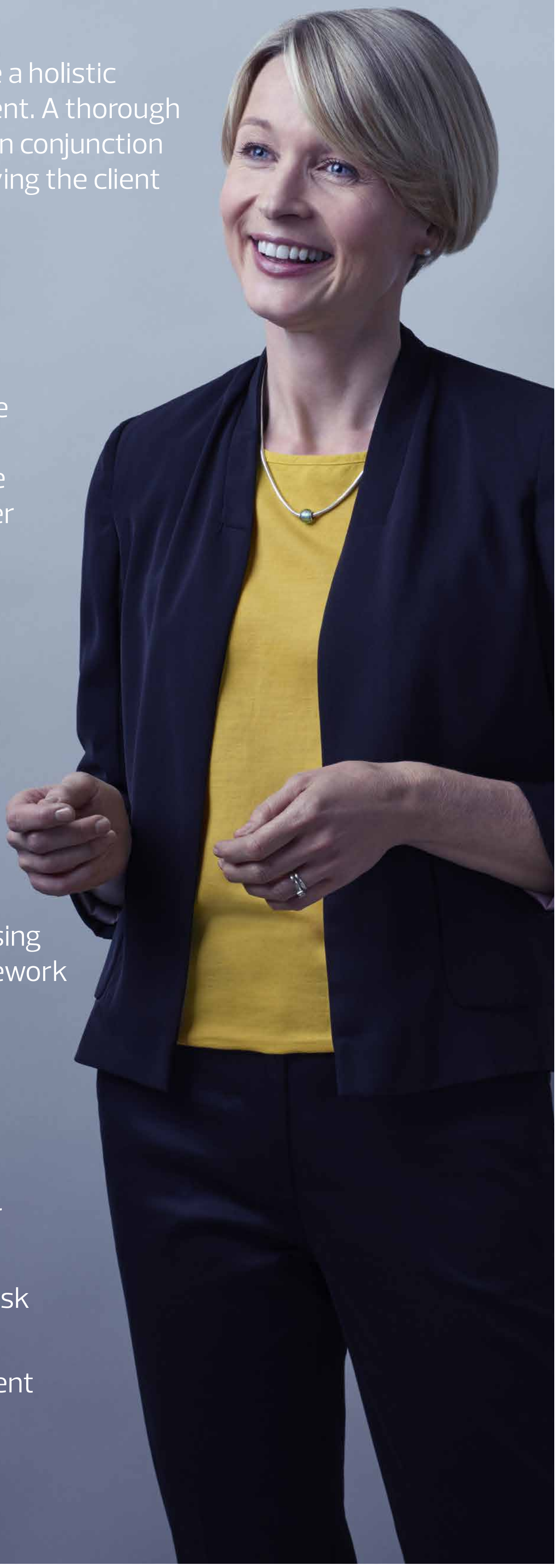
The types of risks that Bill Two aims to manage are:

- **Physical security risks** – This includes risk of harm to people and damage to physical assets
- **Cyber security risks** – Malicious cyber activity is one of the most significant threats facing Australian critical infrastructure assets and can range from denial-of-service attacks to ransomware and targeted cyber intrusions
- **Personnel security risks** – This refers to the 'insider threat' or the risk of employees exploiting their legitimate access to an organisation's assets for unauthorised purposes including corporate espionage and sabotage
- **Supply chain risks** – The reliance on supply chains inherently involves dependencies on other assets or providing other entities with some level of access to, or control of your assets or business' deliverables. As is the case for personnel risk, supply chain risks relate to entities exploiting their legitimate access to, or control of, an organisation's assets for unauthorised purposes or otherwise creating a cascading impact to dependent assets.

SUMMARY

> To address the growing threats to Australia's critical infrastructure, the Federal government has introduced the Security Legislation Amendment (Critical Infrastructure) Bill 2020, subsequently split into two Bills. The bills have expanded the sectors that are classified as critical infrastructure and has introduced additional regulatory requirements per sector and per asset.

How can RSM help you protect your critical OT environment?



When RSM engages with a client, the team undertake a holistic assessment from cyber through to the OT environment. A thorough risk analysis using the appropriate standards is done in conjunction with penetration testing on both sides (IT and OT), giving the client the perspective of what they look like to a hacker.

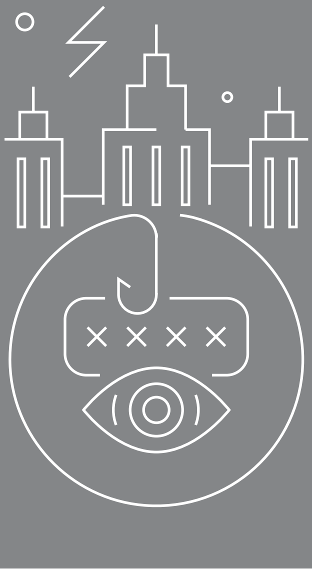
A HIGH-VALUE SNAPSHOT OF YOUR OT CYBER RISK

Our OT Security offering is a simple, fast, and effective snapshot presenting a company's OT exposure in an easy- to-understand manner. The offering covers the following key components to provide a complete cyber security offering to organisations:

- **OT discovery** – complete map of your OT devices along with network visualisation
- **OT Threat Quantification** – complete listing of vulnerabilities and threats applicable to your OT devices with prioritised remedial actions
- **OT Remediation** – provision of an OT security solution and a managed service to ensure ongoing protection and risk mitigation
- **OT Penetration Testing** – cyber security testing using OWASP Methodology and the MITRE Attack Framework

BENEFITS OF THE OT SECURITY OFFERING

- Identification of potentially critical security issues
- Establishment of a baseline for OT security at your organisation
- Quantification of OT risk exposure to assist in OT risk remediation activities
- Complete inventory and map of your OT environment
- Ongoing protection for your OT environment



How the RSM's OT Security offering can protect your business

Our OT Security offering is specifically designed to provide holistic security coverage over your entire OT environment. Our non-intrusive assessment will allow you to document your OT environment in its entirety safely. The offering will also provide an accurate idea of the risks within your OT environment which is a key requirement of the Critical Infrastructure Bill. The remediation service will provide current and ongoing protection for your OT environment.

Who needs the OT Security offering?

The OT Security offering can help your organisation if you need a better understanding of your OT risk exposure or if you are looking at collating a complete inventory of your OT environment for risk management purposes.

Understanding the risk is one thing, but remediating the risk is key.

What we deliver

As part of the OT Security offering, we can deliver the following key components in a non-intrusive manner:

- A complete map of your OT environment
- Comprehensive OT threat quantification with a prioritised remediation plan
- An OT security solution and a managed service to ensure ongoing protection and risk mitigation
- Comprehensive OT Penetration testing and reporting using Offensive security and CREST certified resources

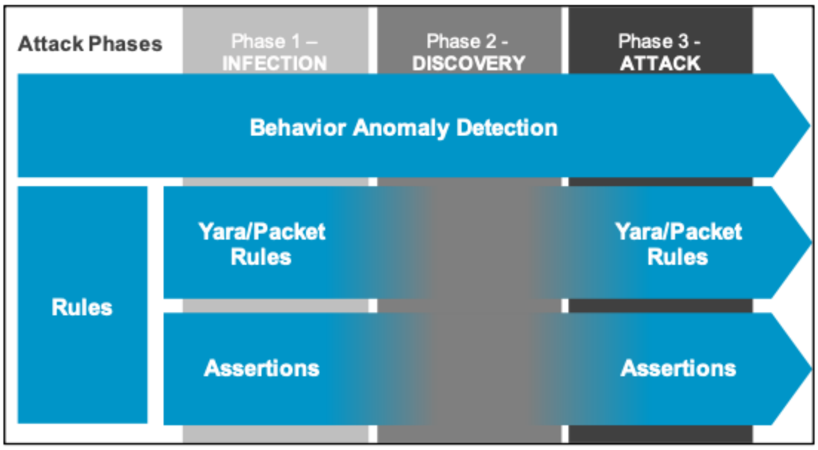
> What this practically means is to approach cyber security in a methodical and thought-out way so that you can understand our key risks and then start treating these risks in a prioritised manner.

How can we get started

Based on our experiences, we recommend starting with a deep dive assessment of your OT infrastructure estate. We work closely with our partner Nozomi Networks to conduct OT environment audits and assessments for a range of end-user organisations. By deploying Nozomi Guardian sensors and management, we can help you understand your environments better by gaining OT asset visibility, vulnerability discovery and threat / risk visibility across the estate.

The Nozomi Guardian appliances secure networks by providing continuous monitoring of cyber security risks, identifying exposure to threats and weaknesses so that cyber security efforts can be focused and prioritised on those areas that are most critical. Guardian provides industrial strength OT and IoT security and visibility with support for hundreds of OT, IoT and IT protocols. Guardian leverages Nozomi's deep expertise in OT protocols for accurate asset discovery, network visualisation, vulnerability assessment, risk monitoring and threat detection in a single application.

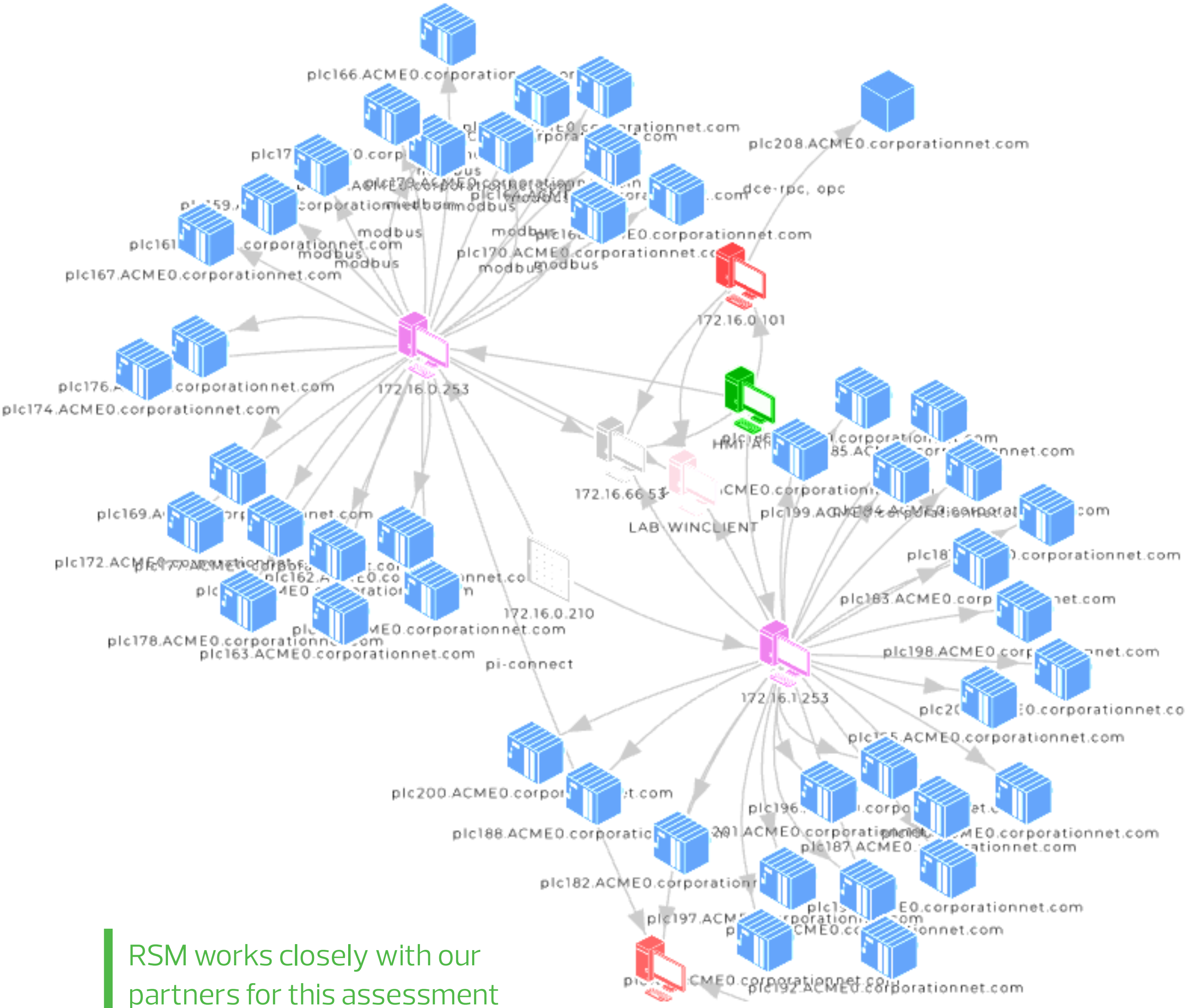
The powerful passive auto-discovery capabilities of Nozomi's Guardian extract the maximum amount of information about nodes, links and assets by monitoring the network through the traffic forwarded through the span/mirror port, performing deep packet inspection, and matching signature profiles to the behaviour that devices have.



> **Cyberattacks are escalating in scale, sophistication, and frequency, exploiting vulnerable systems and weak entry points to target valuable, higher-order infrastructure.**

Darren Booth
Director, Cyber Security and Privacy Services

Guardian's native advanced behaviour-based anomaly detection is enriched with signature and rules-based threat detection. This comprehensive, hybrid approach delivers the best threat detection available for ICS systems. It goes beyond anomaly-only or rules-only analysis, leveraging artificial intelligence to eliminate noise and identify true threats to industrial systems.



RSM works closely with our partners for this assessment following which we typically proceed to help our clients with specific steps that can help manage any identified risks.

WHY RSM

As the largest mid-tier National Partnership in Australia, we differentiate ourselves through an approach that provides:

» **Approach Tailored to You**
» **Leadership Access**
» **Effective Communication**
» **Client Centric Focus**
» **Competitive Fee Structure**

RSM in Australia is a member firm of the RSM Global Network and offers the full suite of assurance services. RSM is a major provider of professional services to the Victorian market and is Australia's largest metropolitan and regional provider of professional services outside of the Big 4 accounting firms. RSM has been in business in Australia for more than 100 years – demonstrating sustained growth through a high quality of service.

Clients engage RSM because we can look beyond the surface and delve into the major factors that affect efficiency and propriety. As the **world's sixth largest accountancy and advisory group**, we have connections to world class expertise and adopt standards that are in accordance with Australian and world best practice.

Our success has been premised on the delivery of a highly personalised service to each client – a principle which has driven our growth over the **past 100 years**. We have **repeatedly won national awards** for the quality of our client service. RSM has excelled over other firms in:

- Depth of team
- Value for money
- Communication and listening
- Reliability
- Independence of advice
- Responsiveness and access to Partners/Directors

100+
RAS professionals in Eastern states

100+
years of service in Australian market

32
offices across Australia

330+
people in the Melbourne office

200
partners and principals nationally

CYBER SECURITY AND PRIVACY TEAM

Darren Booth
Partner
darren.booth@rsm.com.au

Ashwin Pal
Partner
ashwin.pal@rsm.com.au

Riaan Bronkhorst
Partner
riaan.bronkhorst@rsm.com.au

Kaustubh Vazalwar
Associate Director
kaustubh.vazalwar@rsm.com.au

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

rsm.com.au

RSM