14 April 2023
Attn: 2023-2030 Australian Cyber Security Strategy Expert Advisory Board

Re: Nozomi Networks industry feedback on the *2023-2030 Australian Cyber Security Strategy Discussion Paper*

Nozomi Networks welcomes the opportunity to contribute to the 2023-2030 Cyber Security Strategy and commend the effort and focus placed on developing a well-rounded set of policy priorities to establish Australia as the leader in cyber security by 2030.

Nozomi Networks operates at the cutting edge of global efforts to shape decision-making, investment, and action in cyber policy. We work with a range of leading Australian government and critical infrastructure organisations and play a vital role in securing them. Concentrating on enhancing critical infrastructure cyber security, we provide feedback on five key questions from the discussion paper that are particularly relevant to industrial operational technology (OT) and Internet of things (IoT) cyber security.

In 2022, the INCONTROLLER incident highlighted the potential risks of cyber attacks targeting industrial operations. Thankfully, the attack was identified before any operational incidents occurred, showcasing the potential benefits of investing in cyber security solutions specifically designed for industrial operations. As only the fourth known attack using malware aimed at industrial control systems, this event necessitated a highly sensitive response, calling for trust and verification between the industrial control system (ICS) vendor and security research teams.

Australia and many other countries around the world continue to bolster cybersecurity initiatives with the goal of increased trust and verification in mind. Zero Trust has taken on a life of its own with a myriad of definitions and implementation mechanisms from strategy to application. Properly applying a Zero Trust strategy requires studying how technologies interact, what they need from each other, and how to minimise superfluous access to information, command, and control of digital systems.

In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) has issued sector-specific guidelines while simultaneously building trust with industry, to enhance owner and operator input on actions like the rulemaking process for the new Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The European Union is pursuing two new mandates that will provide “an updated and comprehensive legal framework to strengthen both the physical and cyber-resilience of critical infrastructure.”

1. Key Initiatives for Establishing Australia as the World's Most Cyber Secure Nation by 2030

The evolution of OT/ICS technologies has progressed from on-premises connectivity, typically using etherny, to connecting multiple sites and locations, the expansion of Supervisory Control and Data Acquisition (SCADA) architectures, and ultimately to the increasing adoption of cloud technologies. Some sectors are experiencing technological revolutions which are changing the principles of operations, and introducing increasingly smart and connected devices. Others are refocusing their attention on industrial and legacy systems difficult and costly to replace, and shoring up their security approaches in a renaissance of enlightened approaches to a difficult problem set.
Individuals, teams, businesses, and sectors struggle with competing priorities: Connectivity of critical assets to the internet or accessible networks, insecure remote connections, complex and just in time supply chains to name a few. Should they focus on data security? Network security? Devices and endpoints? Does security come before, during, or after cloud adoption and increased automation projects? Despite shared goals and recognised dependence on technology in all aspects of daily life, challenges and constraints hamper the use of existing security frameworks, recommendations, and best practices.

As all sectors continue to reveal cybersecurity gaps, reorient change management, and drive holistic cybersecurity coverage as investments in industrial cybersecurity grow. Focused investments often fall into four main categories:

- **Category 1 – Network Visibility:** If network activity is not monitored in real time, the status of assets is largely unknown, and whether they have vulnerabilities or not, these assets cannot be protected without the necessary visibility into their day-to-day functionality.
- **Category 2 – Vulnerability Management:** Vulnerabilities are not all the same, the degree to which vulnerabilities impact integrity and availability of systems varies by technology, deployment, configuration, and environment.
- **Category 3 – Cyber Threat Intelligence:** Threat actors targeting OT and ICS seek to craft the perfect concoction of capabilities and vulnerabilities that will cause disruption or damage to their target. They can be both opportunistic, highly tailored, or a mixture of both.
- **Category 4 – Lack of Situational Awareness:** Components and connections continue to increase with multiple vendor systems and integrations. Simply having and storing reams of data is not useful for any risk mitigation strategy.

2. Enhancing Government-Industry Collaboration on Cyber Threat Information Sharing

The deterministic, purpose-built nature of OT/ICS ensures that no two attacks on these systems are ever the exact same. The most relevant commonalities from attacks to date include:

- Frequent use of built-in tools, commands, and other items (bins, code libraries, etc.).
- Compromise of systems capable of communicating with field devices or other control systems to deliver impacts.
- Execution of attacks via abuse of legitimate protocols from a compromised endpoint.

The growing number of exploitable vulnerabilities and the great number of potential attack patterns has also revealed three common issues for critical infrastructure:

- Companies and individuals are mostly reacting to security incidents, rather than limiting their severity.
- The looming threat of highly sophisticated, often nation-state level attacks, narrows focus to threat hunting at the expense of other indicators worth investigating.
- Data science in theory is useful for security, but in practice it does not solve for expertise in OT/ICS.

Despite a reluctance by owners and operators to aggregate information, meaningful information sharing requires a vendor-agnostic mechanism for real-time sharing of early warning data. In terms of the threat landscape, there is no way to standardise and correlate threat and vulnerability research produced from the competitive market leaders. Information sharing is lacking trust and verification, and has been siloed into sector-specific, private sector, or government agency-specific mechanisms. This creates single sources of information without much consensus.

Innovation in the ability to provide situational awareness, with trust and verification, will lead the OT cybersecurity future. Many organizations enable tools to gather and store data but fail to analyse data to enhance their mission. Simply having and storing reems of data is not particularly useful for any risk mitigation. Solutions specifically built for OT and ICS will continue to fix security gaps and improve security controls.

The Strategy should consider these unique concerns and challenges for evaluating OT/ICS cybersecurity, preparedness, and resilience.

3. Best Practice Models for Automated Threat-Blocking at Scale

There are limitations to threat intelligence collection, rule application, and analysis for OT/ICS. Because there are no entirely 'cut and paste' tactics, techniques, and procedures (TTPs) from OT/ICS incidents, the only way to secure operations is to include plausibility checks for the systems in play. This involves the categorisation and analysis of process variables for rules-based detections that produce alerts on real world process anomalies, in addition to rules-based data, communications, and potential security anomalies.

Most security companies doing intrusion detection in this space focus on network traffic capture and security monitoring that evaluate and scans for known threat activity. Many include analysis tools to bubble up the trends witnessed through rules-based threat intelligence, to build credible detections and alerts for end users of intrusion detection capabilities. The assumption is that these rules-based detections attribute actions when and where there are enough signatures and signals to allow tools and teams to pinpoint where the attack originated.

Behavioural analysis and anomaly detection for network operations can augment threat intelligence and overall security postures. Anomaly detection can alert on both deviations from normal communications patterns, as well as variables within the process—like sensor readings and flow parameters. This process data can be correlated with communications data to provide actionable intelligence to inform security procedures and reduce overall risk.

The Strategy should consider these unique concerns and challenges for evaluating OT/ICS cybersecurity, preparedness, and resilience.

4. Effective Industry-Guided Post-Incident Review and Consequence Management Model

Where traditional IT assets focus on data at rest or data in transit, ICS/OT systems monitor and manage data that makes real-world changes in with physical inputs and controlled physical actions. According to these differences, specific incident response planning and processes are required, which should include considerations for personal and environmental safety in containing any incident, as well as addressing the unique engineering and system design and network architectures of each situation. According to the 2022 SANS White Paper *The State of OT/ICS Cybersecurity in 2022 and Beyond*, organisations are realizing enterprise IT and ICS/OT environments are not the same. They not only have different types of systems, but also have technologies that are not directly cross-compatible. The missions and risk surfaces differ, and even initial attack vectors, impacts, and approaches to incident response are different.

During an assessment beginning with asset inventory, organisations turn next to understanding the likelihood that potential threat scenarios will be successful in their environments. Unfortunately, the plethora of existing product vulnerabilities in critical operational technology do not translate directly into manipulation of view/manipulation of control scenarios and severity scoring for vulnerabilities is too vague for determining cascading impacts or relevant fallout analysis for a specific facility or operation.

A national strategy can determine what critical infrastructure should not tolerate in OT systems and networks.

The biggest difference when we look at risk assessments for OT versus information technology (IT) is tolerance. Risk tolerance quantification during risk assessments looks very different based on system life cycles, available patches, acceptable system downtime, and the sequencing of maintenance. The tactics, techniques, and procedures of threat actors in cyberspace may or may not find a way to escalate privileges and cause mayhem targeted systems by exploiting vulnerabilities. An organisation might be able to tolerate an unpatched vulnerability in a system, but not something like having shadow it connected to the Internet.

The Strategy should consider these unique concerns and challenges for evaluating OT/ICS cybersecurity, preparedness, and resilience.

5. How Should We Approach Future Proofing for Cyber Security Technologies to 2030?

Unfortunately, there is no single source of truth to turn to for advice across a myriad of national and international guidance and best practices for OT/IoT security. Each company therefore must identify internal teams or champions who act as their own independent advisors. These teams would carry-out literature reviews and consensus mapping, which involves cross-referencing relevant standards, regulations, suggestions, and best practices. Security leaders and teams then must map:

- The status of their security program, risk ownership, and visibility gaps.
- Existing management and mitigation tools, resources, and capacity.
- The development environment of third-party products and security management of suppliers.
- Enterprise content management, data security and PII.
- Operational products and services, hardware, software, IoT, cloud offerings, etc.
- Upstream and downstream supply chain.
- Operational technology and cyber-physical security.
- The sea of available add-on security products.

Risk management has countless starting points with no finish line. Risk tolerance therefore is a cycle of entities mapping necessary security components of their organisation, attempting to understand how those components fulfill various portions of existing standards, regulations, suggestions, and best practices, while hoping compliance regimes measure the right things as necessary to have — which are ultimately industry-specific and thus recreate the cycle. The Strategy should consider these unique concerns and challenges for evaluating OT/ICS cybersecurity, preparedness, and resilience.

About Nozomi Networks:

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimise risk and complexity while maximizing operational resilience.

As partners with our diverse array of critical infrastructure customers, Nozomi Networks focuses on detection and prevention of cyber-physical threats and attacks. We accomplish this with over a decade of perfecting wide industrial protocol coverage and deep packet analysis, continuous monitoring, and mitigation. We deliver visualisation for asset management, vulnerability hunting and scoring, signature threat detection, and next-level situational awareness.

Nozomi Networks is a founding member of the Operational Technology Cybersecurity Coalition, the ISA Global Cybersecurity Alliance the Joint Cyber Defense Collaborative for Industrial Control Systems, and a member of several industry information sharing and analysis centres (ISACs). Nozomi is an In-Q-Tel portfolio company, ISO certified and FIPS compliant solution, and a U.S. Department of Homeland Security Continuous Diagnostics and Mitigation CDM) approved product.

Nozomi's local headquarters are in Sydney, and our regional headquarters are in San Francisco, California and Mendrisio, Switzerland. Our Switzerland office is home to a fully enabled research lab, with water facility and smart city threat and anomaly detection demonstrations. Our Security Research team publishes bi-annual threat landscape reports for OT/IoT.