The real world threats to OT & effective mitigation strategies.

themissinglink

FORTINET

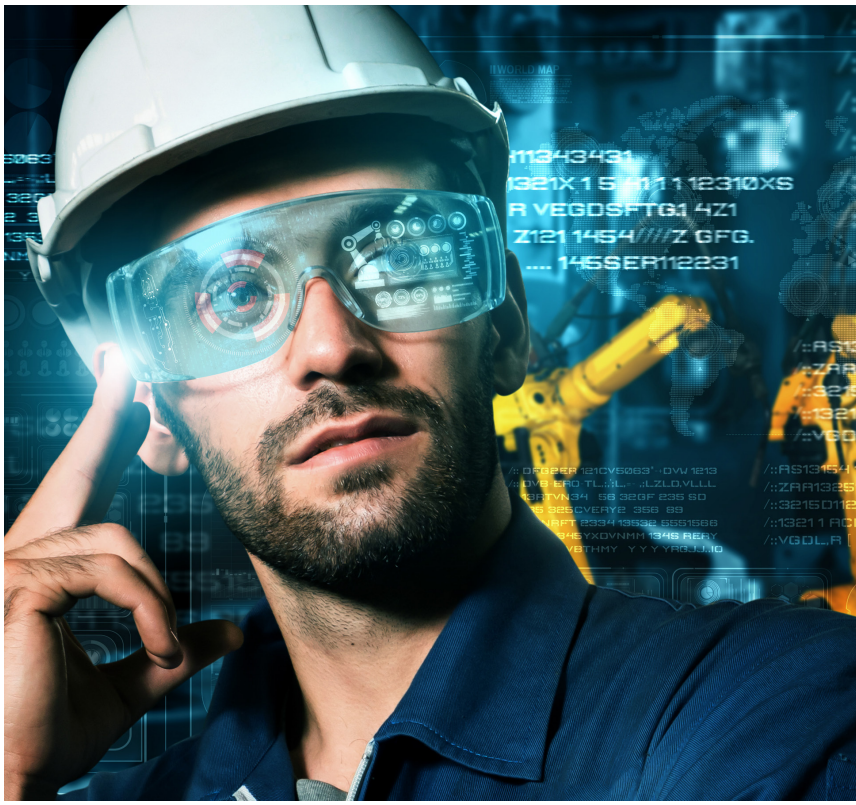
NOZOMI NETWORKS

We live in a rapidly changing world, one in which companies are increasingly introducing sophisticated Information Technology (IT) and Operational Technology (OT) business solutions. **The goal is to find increases in efficiency and productivity that significantly impact the bottom line.**

Why is OT security suddenly a hot topic?

Across industry sectors, we're seeing enterprises blend aging infrastructure, which was never meant to be networked, with new equipment and technology, making maintenance a challenge. The more devices on a network, the greater the attack surface, inadvertently putting data, people, processes and critical infrastructure at risk.

Software exploits designed to infect enterprise IT networks, threatening data and finances, can quickly spread to operational networks and even industrial control system networks. This can cause massive disruption, shut down critical infrastructure, and even threaten human life.



We hear evidence of these attacks all the time. Recent examples include the Oldsmar, Florida breach in which a hacker gained access to the water treatment system and attempted to increase the levels of sodium hydroxide, putting thousands of city residents at risk of being poisoned. Then there was the breach of Norsk Hydro, one of the world's largest aluminium producers, and closer to home, the ransomware attack on LION, which forced a shutdown of production, affecting customers, suppliers and the whole supply chain.

The Missing Link recently connected with notable security leaders; Dovid Clarke, Head of cyber security at Sydney Airport, Jamie Rossato, Information Security Director at LION, Marty Rickard, Customer Success Advisor at Nozomi Networks and Andrew Sheedy, Director of OT Solutions at Fortinet, to discuss the real impact of a cyber attack on every aspect of a business. From data security to day-to-day manufacturing operations, supply chains, and human life, how can enterprises protect themselves from the increasing risks?

A new approach to OT security is necessary

The convergence of IT, OT and industrial control system (ICS) networks is demanding a new approach to security that takes into account every aspect of a business – from its data, people, infrastructure and industrial control system networks, through to its supplier network, manufacturing processes, and distribution.

The need to embed expanded cyber security procedures will become even more critical with the impending rollout of 5G, facilitating an explosion of data from OT, IT and IoT networks. While companies will reap the benefits of quickly collecting, analysing and managing massive amounts of data to gain productivity improvements, hackers too will have ample opportunities to breach networks.

The risks of a breach are no longer limited to data and financial loss … they extend to the disruption of manufacturing processes and supply and even potential injury or loss of human life.

> 5G is going to make what you've deployed from a Wi-Fi and fixed network perspective redundant… suddenly, the manufacturing plant, OT, IT, IoT… it's going to get a huge volume of data that you can actually do something with. Still, you're also going to have all these ingress and egress points (exposing you to attack) that you're suddenly going to have to have a look at.
>
> **Jamie Rossato, Information Security Director, LION.**

The challenges of OT and IT convergence

One of the biggest challenges for enterprises today is establishing a united cyber security strategy that considers the goals and priorities of all aspects of an organisation. This is due to the disconnect between IT and OT executives.

Challenges in the Security Operation Centre

An IT security expert who doesn't fully understand how a plant operates may not realise the flow-on effect of isolating one area of the plant to perform a security upgrade. Performing regular maintenance or emergency patching will result in lost productivity, missed deadlines and even hostility on the floor if not planned appropriately.

Challenges on the floor

On the other hand, without a clear understanding of cyber attack threats, those on the floor may not realise the impact an attack could have on productivity. For example, a rapid shutdown of the plant could result in wasted resources, an inability to meet customer orders and massive reputational and financial damage. Staff may not realise that a cyber attack that disrupts equipment could lead to accidents and even fatalities.

Additionally, they may be unaware that unless precautions are in place to protect infrastructure from cyber attack, the company could be held liable for any damage done to its people or third parties.

The threat of security is real, yet they may perceive the chance of attack as a risk that's worth taking for the sake of continuous production.

Security is not an option; it's a legal requirement

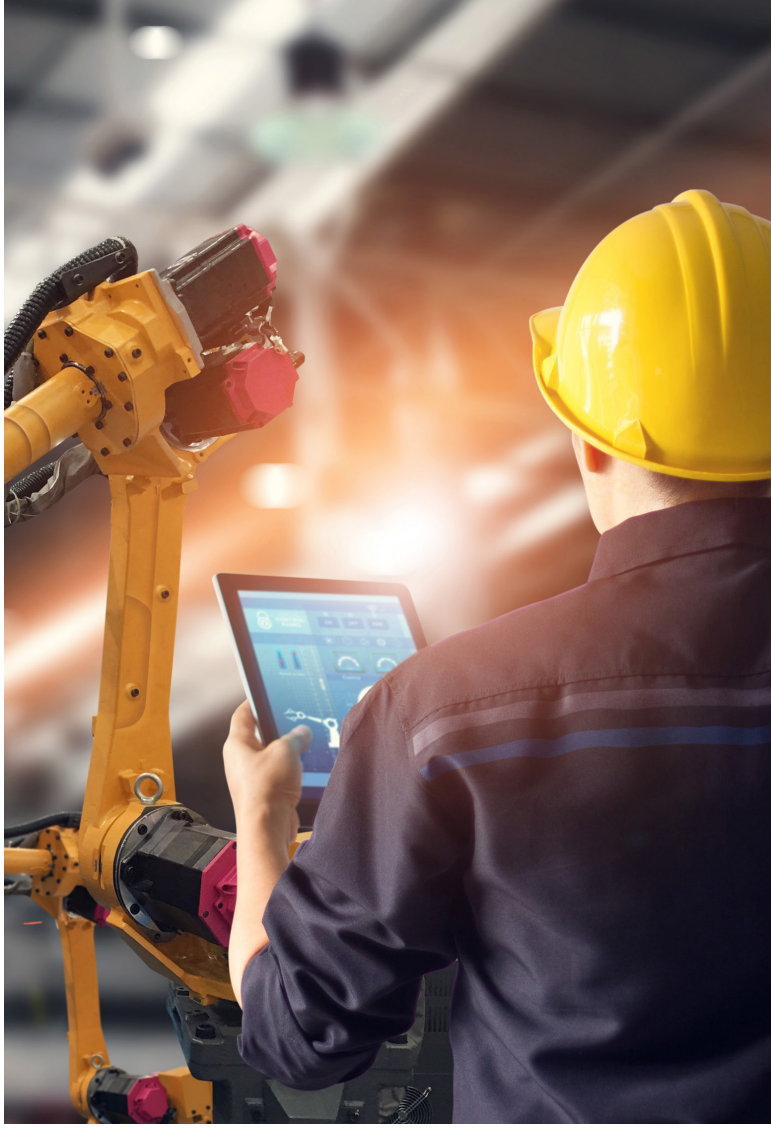
Recognising the increasing risk and impacts of cyber attacks on critical infrastructure assets in the public and private sphere, the Australian Government is currently amending the Security Legislation act.

It is expanding coverage of national security-related essential assets of infrastructure to include 11 critical infrastructure sectors:

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

Enterprises in these sectors with critical infrastructure assets are required to :

1. **Adopt and maintain a critical infrastructure risk management program, to manage and mitigate risks by applying an all-hazards approach**
2. **Comply with mandatory reporting of severe cyber security incidents to the Australian Signals Directorate (within 12 to 24 hours depending on risk)**
3. **In some circumstances, provide ownership and operational information to the Register of Critical Assets.**



Effectively, this makes companies legally obliged to have a cyber security program in place to mitigate the risk of cyber attack and manage the isolation, repair, reporting and reestablishment of processes with minimal disruption.

Indeed, the implications of a cyber attack are far-reaching. If an accident happens, and if a fatality occurs as a consequence of the attack, it doesn't matter how it happened; your organisation will be asked about the steps taken to identify the risk of a cyber event… if you didn't take steps, you would be on the back foot.

So, as part of your cyber security process, you need to identify risks, assess the likelihood of an incident occurring, have steps in place to mitigate, monitor and manage risks, and report an event.

Following an event, you need to take action to change the situation, and when new equipment is installed, or new people come on-site, you must have training in place to ensure everyone understands the processes and controls.

> "I've seen health and safety regulators ask questions around cyber security controls at a manufacturing site… so this is not something to put off to the side… You need to deal with this risk actively."
>
> *Jamie Rossato, Information Security Director, LION.*

> The organisations that are most successful in establishing a cyber security program understand risk and can articulate risk in terms of dollar value (and opportunity cost). They realise the potential cost of an attack on their business and can understand the return on investment in cyber security measures.
>
> *David Bingham, Security Sales Manager, The Missing Link*

Getting the board on board

While some enterprises have found it difficult to focus their board's attention on the need for infrastructure security and even more challenging to justify the necessary expense of doing so, the amended security act should make this a problem of the past.

Once a board understands that they have a legal responsibility to establish a cyber security program, they'll realise that the risk is real, on top of the threat to safety, data, finances, third parties, and production.

So How do you implement a cyber security program?

"When you're talking about protecting your OT and IoT, you're talking about resilience and safeguarding productivity… and all that is achieved through security," Dovid Clarke, Sydney Airport.

Designing and implementing an effective cyber security process to protect your industry infrastructure requires a deep understanding of your manufacturing sites. You need to know where the assets are and who's operating them, the skill sets of the operators and the engineers and their priorities. You need to see the supply chain in action, unfinished goods coming in, finished goods going out. Then, you need to familiarise yourself with the Purdue model for industrial control processes. This industry-adopted reference model shows the interconnections and interdependencies of all the main components within a typical industrial control system, highlighting the levels of protection needed throughout the network.

> One piece of advice I could give any cyber security team is put some overalls on, put some steel-capped boots on, and carry the automation engineer's laptop for a day or a week. See what he does in his job. And if you bridge that gap, if you build a relationship, there's every chance that the engineer will come and sit in the Security Operation Centre next to you for a day, to try and understand what you do.
>
> *Marty Rickard, Customer Success Advisor, Nozomi Networks*

Importantly, you need visibility of all operations so that you can detect when an aspect is out of the norm. You need to understand the impact of a shutdown on every aspect of the plant and the business, and you need to develop a recovery plan to guide the organisation in the event of an attack and shutdown - know the order in which parts of the plant would be restored and validated to minimise disruption.

"I've walked through a few breweries now. The volume and speed at which the manufacturing processes occur really bring home the true impact of disruption. When the general manager for manufacturing said to me, 'All of my sites, all at once, stopped working,' I realised that hundreds of thousands of bottles on the line just had to be thrown off. It's a huge impact. Huge impact." Jamie Rossato.

You can only gain a full understanding by getting to know the person who starts the systems up from the dark and closes them down. Work through the processes with this person; they will be your best advocate once you explain what you're trying to achieve and why… and most importantly, ensure your cyber security process is clearly documented.

"Get it documented, understand it. And, yeah, identify, identify, identify. If you can't see it, you can't protect it. So go out and find it all," Marty Rickard.

Invest in intelligent OT/IoT security

Alongside clear processes, enterprises need to be equipped to monitor, detect and respond to incidents, then, importantly, be able to report them in line with current legislation. This is something global cyber security vendor Fortinet offers.

Recognised in the Gartner Peer Insights Customers' Choice 2021, the company's portfolio of tools and technologies enables coordinated threat detection and policy management across the entire digital attack surface, even as environments increasingly converge and across edges, clouds, endpoints, and users.

To stay abreast of the convergence of IT, OT and IoT, you've must have good sources of information, something most companies don't have internally, Marty Rickard points out. That's why Nozomi Networks has experts doing this on enterprises' behalf, providing the intel required to ensure their security operations team can "point their guns in the right direction".

With increasing convergence presenting greater threats, vulnerabilities, risks and anomalies, Marty says the value of being able to monitor networks with speed and expertise will continue to grow. To this end, the company is building artificial intelligence and machine learning to detect activity outside the norm - this means customers can be alerted to risks with certainty, and in doing so, avoid wasting time chasing false positives.

At The Missing Link, we work with companies like Fortinet and Nozomi Networks to design and implement holistic cyber security processes that protect companies' IT, OT and IoT within an increasingly convergent world. Recognising the challenges of meeting disparate priorities across different areas of organisations, our certified security experts partner with organisations and take the time to understand all processes at the deepest level, their objectives and budget.Then we create a customised cyber security plan that protects their data and infrastructure from attack, equips them to respond to attack and enables them to minimise the disruption to their processes in the event of an attack.

Not investing in cyber security is no longer an option - it doesn't make sense financially, legally or logistically. As Jamie Rosatto says, "There's no easy sugar hit once an organisation has been breached; you're really on the essential journey to protect multi-millions of dollars in value by uplifting your organisation - IT, OT and personnel".

Contact Us

1300 865 865

sales-tml@themissinglink.com.au

themissinglink.com.au

themissinglink

FORTINET

NOZOMI NETWORKS