Employ Innovative Strategies To Safeguard The Heart of Industrial Manufacturing From Evolving Cyber Threats

At the heart of the industrial complex, a manufacturing plant, much like any other, was bustling thanks to its well-orchestrated production lines and supply chain workflows. Unbeknownst to them a silent intruder, Triton malware, had breached the manufacturing plant's critical control systems with one precise intention... manipulate key safety mechanisms.

Triton sought to compromise the efficiency of the manufacturing plant. As well as this, however, by manipulating critical OR essential safety mechanisms, Triton was able to pose a direct threat to the physical safety of equipment and people working on the plant floor.

Unlike traditional IT systems, incidents such as Triton underscore that cyber threats now pose a risk to everything in the physical world as well as the digital ecosystem, reaching into the fabric of our critical operational functions that can lead to severe consequences.

Vulnerable Supply Chains

The supply chain is an essential construct to industrial manufacturing companies, where even simple delays or failures in logistics can have costly impacts on the business.

Maersk is one example where ransomware known as NotPetya caused millions of dollars in damage and widespread subsequent damage after shipping containers were left stranded and logistics disrupted. The interconnected nature of our supply chains left cascading effects of this malware on industrial operations.

The collateral damage emphasised the urgency for manufacturers to fortify their cyber defences, recognising that threats to one element (such as a supplier) in the ecosystem can become a threat to many others within it.

Physical World Zero-Days

Consider a manufacturing plant that fabricates integrated circuits used in computing machinery. Let us assume there was a compromise of one or more sensing devices used for critical measurements, causing them to be slightly offset or entirely incorrect. Also, consider the possibility of these devices being calibrated incorrectly by a technician working on the plant floor.

One or more simple measurement errors in even a single batch of circuits that were manufactured in this plant can cause significant financial loss. These circuits will be shipped from the manufacturer to suppliers, where they will eventually be installed and malfunction. By this point, many other batches may have been made, and financial implications extend from recall costs but potentially to malfunctions of devices in other domains.

It is critical to ensure in these domains that accuracy and precision, regardless of the origin of this threat, are also accounted for.

Aftermath

In the aftermath of these two pieces of malware, the manufacturing industry underwent an almost immediate paradigm shift in its approach to cybersecurity. Safeguarding operational technology is now paramount, as in connected environments where digital and physical environments interact – safety becomes a security concern.

As the cyber threat landscape evolves, with constant risk pressures, manufacturing companies must employ a holistic security strategy to retain resilience and ensure the integrity, safety and continuity of their critical business operations.

Strategies for Achieving Cyber Security Resilience

Compliance with standards and regulations

Adhering to industry-specific cybersecurity standards and regulations can establish a baseline for good security practices. Key examples include:

- ISO27001
- ISA/IEC 62443

By conducting regular compliance audits, you can ensure alignment with these established standards and identify areas of improvement.

Sapphire has extensive experience and expertise to help align you and your operations with compliance standards, swiftly identifying vulnerabilities and gaps and offering tailored solutions to maintain alignment.

> Did you know that Sapphire has a 100% ISO27001 pass rate, enabling you to achieve certification on the first attempt?

OT Asset Identification/Discovery

This refers to approaches that can identify, categorise, and manage all the components within your industrial environments. OT assets typically include a wide assortment of devices and systems, such as programmable logic controllers (PLCs), human-machine interfaces (HMIs), actuators, sensors, and other hardware and software that control and monitor your critical operational processes.

Do you know how many assets you have and are they all robust to compromise?

Sapphire's OT solutions can help you actively seek and identify devices in your OT environments and profile them so you can learn more about each of your devices. Creating a detailed inventory of your environments and continuously monitoring your critical assets is essential.

Endpoint Protection and Access Controls

Implementing robust measures for endpoint protection can help safeguard your devices connected to critical networks. Furthermore, enforcing stringent access controls to limit unauthorised access and prevent lateral movement across and within networks. Sapphire can help you with identity and access management, implementing robust access controls and managing your endpoint devices. Also benefit from our EDR/XDR solutions to better your security monitory capabilities.

Security Awareness Training

One of the most significant risks to the security of your organisation is your people. Sapphire's managed security awareness training can equip you with bespoke, actionable skills to prevent and mitigate threats that start with your employees.

Cultivate a security-first and safety-first culture among your colleagues within every department to promote a sense of responsibility and accountability.

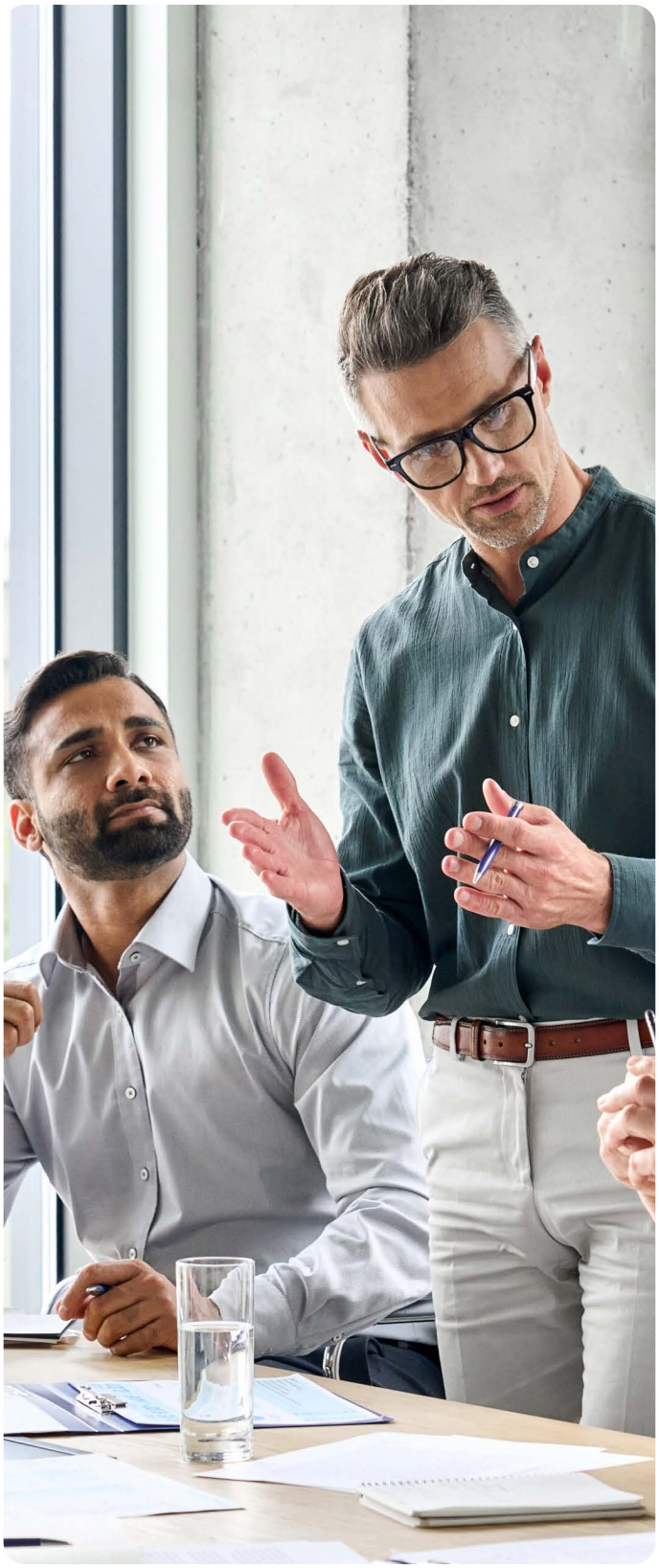
Third-party Risk Management

Ensure you review the security of your third-party suppliers and the potential risks they may pose to your organisation.

Benefit from Sapphire's automated third-party risk assessments and timely reporting of your third-party risks, which can help you with readiness in the face of unforeseen attacks such as those previously observed with the likes of TRITON and NotPetya.

Internal/External Audits

Because the threat landscape is changing rapidly, you have to ensure your security protocols are up-to-date to protect you against even the newest threats. As well as this, you must remain compliant with new and changing regulations in your sector. Sapphire's audit services can help guide you through the testing of your security protocols and critical business functions to ensure you are compliant and free of potential security flaws. Key examples include compliance to international standards such as ISO 27001 and ISA/IEC 62443.



To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Sapphire's Service Offering

Service /Offering	Introductory	Foundations	Intermediate	Advanced
NCSC Guidelines	✓	✓	✓	✓
Standards Compliance Review	✓	✓	✓	✓
Gap Analysis	✓	✓	✓	✓
Security Improvement Planning	✓	✓	✓	✓
Security Awareness & Training	✓	✓	✓	✓
Procedure & Policy Review	✓	✓	✓	✓
Network Configuration Review	✓	✓	✓	✓
Firewall Security Checkup	✓	✓	✓	✓
Framework Review (CyberEssentials, GovAssure)		✓	✓	✓
Information Security Management		✓	✓	✓
Authentication Review		✓	✓	✓
Business Continuity Planning		✓	✓	✓
Disaster Recovery Planning		✓	✓	✓
Incident Response Planning		✓	✓	✓
IT/OT Asset Discovery		✓	✓	✓
Identity & Access Management Review		✓	✓	✓
Threat Assessment		✓	✓	✓
Penetration Testing		✓	✓	✓
Internal/External Audit		✓	✓	✓
Threat Intelligence			✓	✓
Vulnerability Management			✓	✓
Third-Party Risk Management			✓	✓
IT/OT Consultancy			✓	✓
MXDR & Endpoint Management				✓
CISO as a Service				✓
Red Teaming				✓
Breach Attack Simulation (BAS)				✓
SIEM & SOC Advisory Services				✓

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001