Nasstar

Securing smart industry

Mapping vulnerabilities in manufacturing, logistics, energy & utilities

Whitepaper

2025

Contents

Introduction

Capabilities unlocked by IIoT (Industrial Internet of Things) and IT/OT (Operational Technology) integration deliver a range of benefits, from operational optimisation and carbon reduction to continuous uptime, more informed decision-making and enhanced cost efficiency.

However, advanced systems and network integrations can also translate into a greater surface area for cybercriminals to target. For this reason, manufacturing, logistics, energy, and utilities (MLEU) organisations must ensure that their security postures are evolving in line with digital ambitions.

"It's well known that digital transformation brings numerous benefits and efficiencies to MLEU organisations. However, what's often overlooked are the potential cyber security risks and technological vulnerabilities that could impact a business.

By combining Fortinet and Cisco's advanced technologies with our expertise, we help build secure and adaptable networks that empower businesses to focus on what matters most - growth and innovation, knowing their systems are optimised and well-protected."

Leigh Walgate
Managing Director, Secure Networks at Nasstar

Manufacturing, logistics, energy, and utilities

Universal cyber security vulnerabilities

With almost one third of organisations in the energy and industry sectors recording at least six intrusions in 2024, cyber security incidents are becoming increasingly problematic. Data suggests[1] that advanced technologies are contributing to the growing complexity of managing certain threats to which all MLEU organisations are vulnerable.

Third-party software

can introduce vulnerabilities if not properly secured. Adopting endpoint protection and thoroughly vetting vendors will significantly reduce risk for MLEU organisations.

OT ransomware

can encrypt critical operational systems, causing significant disruption and expense. Implementing network segmentation helps contain the impact, while maintaining regular back-ups ensures data can be restored without paying a ransom.

Insider threats

from human error or sabotage, are a common source of security breaches. Regular audits and close monitoring of user activity are essential first-steps towards mitigating these threats from within.

Inadequate threat detection

especially at IT/OT integration points such as sensors and actuator networks, can leave MLEU organisations exposed. Advanced monitoring and proactive threat detection tools must be deployed to ensure adequate vigilance.

Default security credentials

including factory-set passwords on IIoT devices, offer cybercriminals an easy way in. Systems should be protected through strong password policies and bolstered by regular password changes.

Shadow IT

refers to an organisation's use of software, hardware, or services that are not approved, managed, or supported by the IT department. Robust policies, procedures, and tools are required to manage Shadow IT and prevent security breaches from harming operations, compliance, and reputations.

Manufacturing

Vulnerabilities

Manufacturing companies cannot afford to let vulnerabilities slip under the radar. Breaches often bear harmful repercussions, affecting productivity, compliance, safety, reputations, and revenues.

Human error

is widely regarded to be a pivotal factor in enabling cyber security intrusions[2], and manufacturing is no exception to this trend. One of the most effective ways for manufacturers to protect themselves is through regular training to ensure employees follow best practice.

Legacy equipment

so often lacking in modern security features and difficult to update, is a common vulnerability for manufacturers. Network segmentation, compensatory controls, and phased equipment upgrades offer enhanced protection.

Poorly segmented networks

particularly across IT and OT systems, may allow malware to move freely. Firewalls, virtual local area networks (VLANs), and proactive monitoring tools can help to identify and isolate this threat, preventing such intrusions from snowballing out of control.

Third-party access to critical systems

may expose manufacturers to ransomware or intellectual property theft. Manufacturers should conduct careful vetting of their vendors and implement strict access controls and endpoint monitoring to protect themselves from supply chain risks.

Unsecured IIoT devices

such as robots or advanced sensors, can be targeted by hackers or saboteurs. Robust authentication and encryption standards must be maintained to safeguard these systems.

Logistics

Cyber security vulnerabilities

The logistics sector is modernising rapidly, with technologies transforming how businesses handle everything from resource planning and inventory management to customer data. With increasing digitisation comes increasing potential for cybercrime, which can have devastating results.

Connected fleet systems

such as GPS and telematics are vulnerable to hacking which can wreak operational havoc upon logistics businesses. Encryption of communication channels and careful monitoring for anomalous activity help protect connected fleet systems.

Warehouse management systems

(WMS) and Enterprise Resource Planning (ERP) software deliver impressive efficiencies for logistics companies. But these systems are also enticing targets for cybercriminals. Robust access controls, regular updates and penetration testing all help to make vendor applications more secure.

IoT-enabled asset tracking

can be compromised, allowing criminals to identify, locate and steal high-value cargo. Advanced encryption and device authentication are effective ways of mitigating this threat.

Phishing and social engineering

scams are frequently leveraged by cybercriminals to access sensitive information. Logistics businesses can protect themselves through thorough employee training and awareness programmes, as well as email filters and frequent system backups.

Endpoint devices

such as handheld scanners, are often configured with default login credentials, offering opportunistic hackers an easy route into logistics networks. Device updates and best-practice password protocols should be leveraged to prevent infiltration.

Energy

Vulnerabilities in technologies

The threat level for energy sector organisations is rising[3]. Not only is digitisation increasing the surface area for cyberattacks, hybrid warfare fuelled by geopolitical tension puts critical infrastructure in the crosshairs, further heightening risk.

Remote access monitoring

is highly beneficial in the energy sector. However, weak protocols can enable unauthorised access to control panels for equipment and infrastructure, potentially leading to grid instability or data breaches. Multi-factor authentication and secure VPNs help make remote systems more secure.

Distributed denial-of-service

(DDoS) attacks targeted at energy service providers overwhelm systems, disrupting service availability. These attacks can impact customer trust and critical operations. Traffic filtering and network redundancy measures help ensure service continuity in the face of such attacks.

Critical infrastructure

like power stations and gas pipelines rely on real-time monitoring for security. However, if compromised – for example, through sensor tampering – intrusions may go unnoticed, leading to severe consequences. Advanced analytics and machine learning can enhance sensor networks, delivering automated alerts to detect anomalies early and prevent issues from escalating.

IoT-Enabled smart meters

are designed with security in mind but are vulnerable to manipulation. Billing fraud[4] and load oscillating attacks[5] both represent tangible risks. Constant monitoring and encryption of smart meter data are necessary steps towards mitigation.

Utilities

Cyber security vulnerabilities

From water treatment facilities to smart grids, cyber vulnerabilities in utilities demand urgent attention to ensure service continuity and public safety.

Unpatched firmware

for example on IoT devices within utility systems, may allow malicious actors to disrupt operations. Regular updates to firmware provide important new security features, whilst vulnerability scans can help to highlight weaknesses that need to be addressed.

Water treatment facilities

can be targets for hackers who may exploit weak process control systems to manipulate equipment. Advanced access controls and process log monitoring helps mitigate these risks.

Smart grids

if not protected through encryption and intrusion detection systems, are prone to intrusion. Compromised smart grid communication systems could potentially lead to blackouts, and so must be safeguarded.

Data interception

made possible through unencrypted communication channels, may expose sensitive grid control data to cyberthreat actors. Encrypting all transmissions ensures data integrity and prevents unauthorised access.

Distributed energy resources (DER)

are small scale energy systems operating outside of the central grid. The integration of DER into utility networks can expose vulnerabilities, for example if connections are poorly secured. Strict security protocols and regular audits help protect these systems.

Conclusion

From efficiencies to improved quality control, decision-making, sustainability, and even security, digital transformation delivers benefits that MLEU organisations must embrace to ensure future success.

However, enhanced cyber security is not a given. As digital surface area increases, so to do potential vulnerabilities across networks, infrastructure, and systems.

If MLEU organisations fail to develop their security postures in proportion to the evolving risk, the likelihood of costly breaches or incidents is drastically increased.

Organisations must put themselves on the front foot. A proactive approach, dynamic strategies and expert support all come together to make this possible.

"Nasstar's experts understand your challenges, offering transformational solutions that deliver dramatic improvements. We'll help you enhance security and productivity, drive greater efficiency and enrich the employee and customer experience. Speak to us about unlocking more value from your technology."

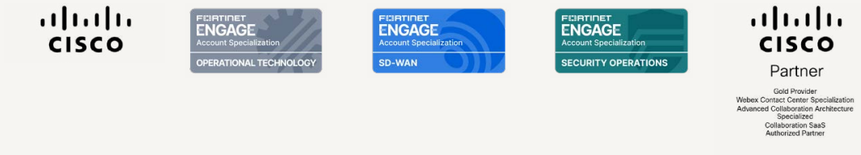
Mike Ayres
Commercial Director, Nasstar

Transform your operations. Secure your systems.

Introducing Nasstar

Nasstar is the trusted digital transformation partner for manufacturing, logistics, energy, and utilities organisations. We specialise in handling the risk and complexities of smart industry, enabling our clients to reap the rewards.

- **Stay a step ahead** of cybercriminals withproactive security
- **Adopt cloud computing** for agile, scalable operations
- **Embrace automation, IIoT, ML and AI** for cost-saving and control
- **Enhance connectivity** for greater visibility
- **Leverage big data analytics** for better decision-making



Get in touch

We’d love to hear from you

Head office
Melbourne House
Brandy Carr Road
Wakefield, West Yorkshire
WF2 0UG

Telephone
0345 003 000

General enquiries
salesenquiries@nasstar.com

Website
www.nasstar.com

Wherever you are on your digital transformation journey, Nasstar can help you get more from your technology.

Prepare for tomorrow.
Book a free consultation today.

1. 2024 State of Operational Technology and Cybersecurity Report www.fortinet.com/resources/reports/state-of-ot-cybersecurity
2. 2024 Threat Hunting Report https://go.crowdstrike.com/2024-threat-hunting-report
3. Infosecurity Magazine www.infosecurity-magazine.com/interviews/anjos-nijk-securing-electricity
4. https://www.theguardian.com/technology/2016/dec/29/smart-electricity-meters-dangerously-insecure-hackers
5. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10098782&tag=1

Nasstar

Securing smart industry:

Vulnerabilities in manufacturing, logistics, energy & utilities.