Nasstar

Ebook

Five critical cyber vulnerabilities in energy and industry

2025

Introduction

With increased digitisation, comes increased ‘digital surface area’ – meaning increased risk.

To say that digital transformation represents an ‘opportunity’ for manufacturing, logistics, energy, and utilities (MLEU) is an understatement. IIoT (Industrial Internet of Things), IT/OT (Operational Technology) integration, automation, machine learning, and AI can enhance efficiency, productivity, scalability, and profitability.

Digital transformation is what will separate those that thrive from those that are left behind.

However, embracing smart industry is far from straightforward. One key challenge is that with increased digitisation comes increased ‘digital surface area’ – which in turn means increased risk.

The research tells a story. Almost one third of energy and industry organisations recorded at least six intrusions in 2024. 73% of those surveyed reported intrusions affecting OT systems.

Just as organisations must evolve to keep pace with new technologies, security measures must also evolve according to new threats.

The good news is that digital transformation can deliver benefits without increasing the risk of cyber threats. With the right expertise, targeted investment, and a clear strategic vision, smart industry solutions will prepare your business for what comes next.

This e-book highlights five of the most critical vulnerabilities in MLEU right now. It offers insight into how your organisation might be exposed and, most importantly, how you can protect it.

OT Ransomware

Developments in OT and its integration with IT systems are key features of MLEU's digital transformation. Unfortunately, OT is also a key target for cybercriminals.

Typical OT ransomware may be used to encrypt critical operational systems. In manufacturing, this could halt production, while in the energy sector it could result in blackouts.

Disruption caused by OT ransomware can be devastating – but that's only half the story. Perpetrators then demand extortionate ransoms, which victims may find they have no choice but to pay.

Network segmentation is an effective way to contain ransomware, preventing it from spreading to other systems. Advanced monitoring and proactive threat detection are also important steps towards mitigating risk, while frequent back-ups mean data can be restored without yielding to an attacker's demands.

Network segmentation is an effective way to contain ransomware, preventing it from spreading to other systems.

Insider threats

Human error is one of the leading causes of security breaches. Research findings vary, but studies suggest anything from 55% to 95% of incidents are attributable to users. Whatever the true extent of human culpability, error is certainly a significant factor.

While social engineering and phishing aren't technically 'insider threats,' people who fall victim to such scams often make mistakes that leave themselves and the organisation exposed.

Sabotage – intentional malicious acts such as deleting or corrupting data, installing malware, or introducing system vulnerabilities – represents another potential threat from within.

One of the most effective things MLEU organisations can do to reduce human error is to implement regular training. This ensures that employees know the risks and follow best practice security procedures. Alongside training, proactive measures such as audits, email filters, frequent system back-ups and close monitoring of user activity also help mitigate insider threats.

Legacy systems

Many systems throughout the energy and industry ecosystem have been in use for years or even decades. Such legacy systems are often difficult to update, which invariably means they lack the necessary security features to keep attackers at bay.

Moreover, their integration with modern systems can create additional vulnerabilities, as outdated protocols may not align with contemporary security practices.

While phased upgrades are planned and implemented, network segmentation and compensatory controls help to protect outdated infrastructure.

Regular vulnerability assessments and proactive monitoring are also essential to identify weak points, ensuring that legacy systems remain as secure as possible during the transition to modern alternatives.

To ensure that legacy systems remain secure during transition, regular vulnerability assessments and proactive monitoring are essential.

Default security

Default access controls, including factory-set passwords on IIoT systems and endpoint devices, provide cybercriminals with an easy way in.

There are many ways that these vulnerabilities can be exploited. For example, in the logistics sector, threat actors may target handheld scanners to infiltrate a network and inflict operational disruption, or to facilitate the interception and theft of valuable cargo. In utilities, hackers may leverage default log-in credentials to access and destabilise critical infrastructure.

To bolster security, default passwords should be changed immediately when setting up new systems or equipment and after any factory resets. Additionally, strong password policies must be enforced, including regular password updates to ensure ongoing protection.

Unauthorised, so-called ‘shadow IT systems’ pose significant risks to MLEU organisations.

Third-party vendor applications and shadow IT

Unauthorised or inadequately secured software, hardware, and services pose significant risks to MLEU organisations.

Shadow IT – systems installed and used without adherence to security protocols or oversight from the IT department – is a common way organisations become exposed. Similarly, third-party vendor applications can introduce vulnerabilities if not properly assessed.

To protect against network breaches, non-compliance, operational disruption, and reputational damage, MLEU organisations must tread carefully.

All third-party applications should undergo a thorough vetting process, while robust policies and procedures are essential for managing shadow IT. Proactive monitoring and clear governance further safeguard systems against inadequately secured technology.

Nasstar can dramatically enhance your resilience, giving you total peace of mind, as we ensure you’re fit for the future.

Transform your operations. Secure your systems.

Introducing Nasstar

Across energy and industry, organisations must embrace dynamic, proactive strategies to ensure their security postures are evolving in line with their digital ambitions. But with new threats and opportunities emerging all the time, keeping your organisation on the front foot is easier said than done.

Nasstar can help. We are the trusted digital transformation partner in manufacturing, logistics, energy and utilities. We specialise in handling the risk and complexity of smart industry adoption, allowing you to reap the rewards.

Get in touch ↗

- **Stay a step ahead** of cybercriminals with proactive 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

Cisco

Fortinet Engage Account Specialization – Operational Technology

Fortinet Engage Account Specialization – SD-WAN

Fortinet Engage Account Specialization – Security Operations

Cisco Partner
Gold Provider
Webex Contact Center Specialization
Advanced Collaboration Architecture Specialized
Collaboration SaaS
Authorized Partner

Nasstar