ptc®

Secure OT Networks through Industrial Connectivity Before Disaster Strikes

The Common Challenges and Rising Stakes of OT Cybersecurity

kepware®

WHITEPAPER

Organizations are woefully unprepared for operational technology (OT) security threats—but most don't realize it until it's too late.

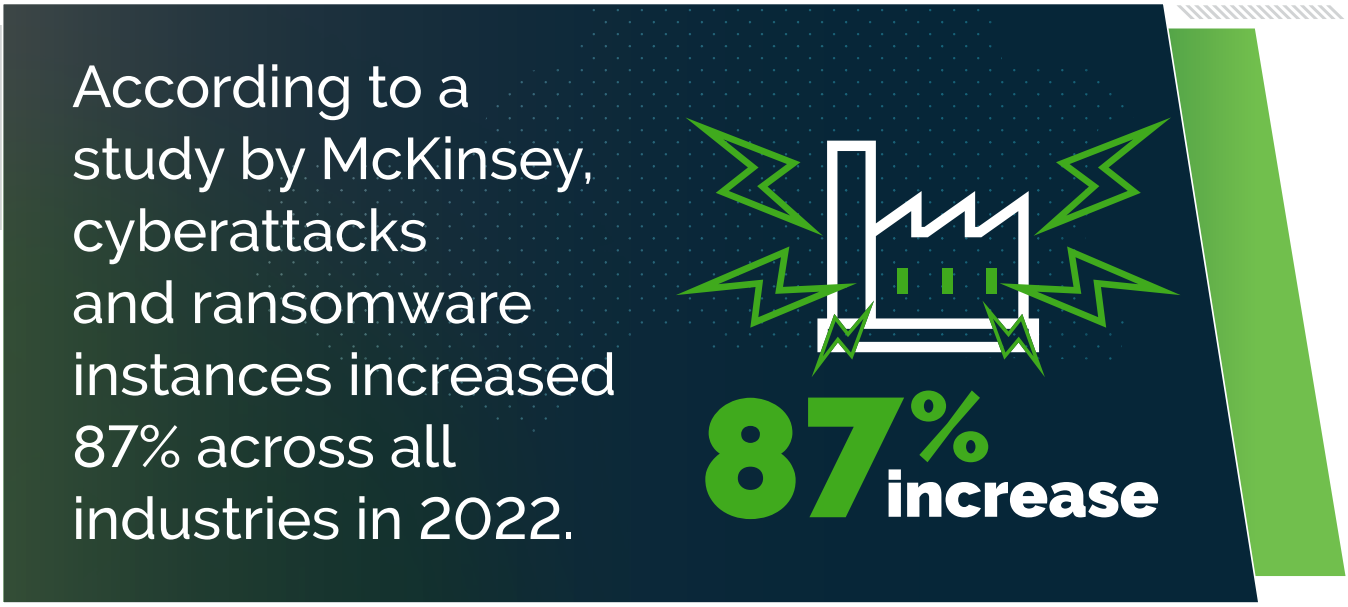
Take the example of Norsk Hydro, a multinational aluminum manufacturer that was forced to shut down operations in the face of a ransomware attack across its systems. They opted not to pay the ransom, but the interruption to their operations cost them nearly $75 million. The news is rife with examples like this, and regulators have taken notice and are forcing manufacturers to act. But safeguarding OT assets can be challenging amidst competing business priorities, a broad attack surface, and unclear ownership.

Ransomware has become more common for manufacturers, causing shutdowns, financial losses, and logistical nightmares. According to a study by McKinsey, cyberattacks and ransomware instances increased 87% across all industries in 2022. ICS Strive, an online database of OT attacks, recorded 68 known attacks on OT and ICS networks in 2023, impacting more than 500 physical sites.

The increased frequency of ransomware can be attributed to volatile geopolitical conditions. Bad actors are increasingly targeting critical manufacturing supply chains and infrastructure as tensions between countries escalate, compromising intellectual property, production continuity, and safety. They also create substantial safety concerns for workers, assets, and the environment.

While threats, industry, and technologies are evolving, so are compliance regulations. Governments are moving quickly to keep pace with modern malware techniques through policy change and enforcement. Manufacturers must keep themselves informed on the latest regulation changes to safeguard their operations from these threats or else face legal consequences and operational disruption.

The waters of IT security have always been treacherous, and they have only become more so with these new waves of OT vulnerabilities.



WHY NOW?

Given the increasing frequency of attacks and the criticality of the manufacturers at risk, regulators have taken notice and are acting quickly to protect critical infrastructure. In January 2023, the European Union (EU) released new directives to keep pace with digitization and increasing threats. The scope and financial impact of Network and Information Systems Directive 2 (NIS2) have a global impact.

NIS2 applies to any organizations that:

- Offer services or operate in the EU
- Employ over 50 people or generate at least €10 million in revenue
- Provide essential goods
    - Digital Infrastructure
    - Energy
    - Finance
    - Health
    - Public Administration
    - Space
    - Transport
    - Water Supply

Key changes include:

- Extended security requirements
- Expanded classification of "critical infrastructures"
- Stronger incident reporting requirements
- Greater focus on supply chain security and international cooperation

EXPECTED IMPACTS AND COSTS:

- **Increased** company and executive accountability
- **Steeper** financial penalties for noncompliance
- **Public disclosure** of breaches, damaging brand reputation
- **More resources** allocated to OT security

Member states have until October 17, 2024, to codify NIS2 into national law. Afterward, organizations will have 21 months to get their operations fully compliant. This has a global impact on the industrial and manufacturing market, as OT security resources may become scarce as compliance deadlines draw closer.

With limited resources and evolving threats, it is urgent for all to examine the state of their OT security.

OT SECURITY OBSTACLES

Manufacturers are painfully aware of OT threats and that security needs to be a top priority—so why are so many slow to meet these evolving security requirements? Building and maintaining a secure IT-OT ecosystem poses a series of challenges, including but not limited to:

Legacy Systems and Hardware

Many manufacturing facilities rely on legacy equipment and systems that were not designed with modern security protocols in mind. Updating or replacing these systems can be complex and costly. However, securing the existing assets while enabling seamless integration with newer technologies is no simple feat.

Vulnerable, Outdated Protocols

Communication protocols within any given factory are often inconsistent and outdated. Normalizing data across varied protocols is challenging, especially across an entire enterprise. Vulnerabilities in these protocols can be exploited by malicious actors.

Connected Assets and Insecure Remote Access Procedures

As manufacturing environments become more interconnected, the attack surface for cyber threats increases. Connected assets (e.g., sensors, control systems) provide valuable data but also serve as potential entry points for attackers. Insecure remote access procedures can compromise the entire system. Balancing the need for connectivity with robust security measures is crucial.

Competing Business Priorities

Manufacturers must strike a delicate balance between productivity, efficiency, and security. While optimizing production processes, security measures can sometimes take a back seat. Business leaders must recognize that OT security is not just a technical concern but critical to business continuity and resilience.

Unclear Roles and Responsibilities

Defining clear responsibilities becomes vital to your security strategy, where IT and OT technologies interconnect IT and OT operations. Company-wide policies can be insufficient, particularly for advanced technologies. When specific devices (such as digital twins) fall under both IT and OT, their security may be fragmented or overlooked.

While these hurdles to improving security are hardly trivial, they are also part of the reason lagging manufacturing OT environments are such attractive targets for digital attacks. The good news is that there are clear paths that any manufacturing organization can follow to begin the process of meaningful OT cybersecurity improvements—regardless of their shop floor infrastructure.

UNITING IT AND OT

The first step in reducing cybersecurity risks and addressing the vulnerabilities outlined above is to think critically about which group is best equipped to solve each challenge while considering the overall governance structure. Many companies employ CISOs (chief information security officers) to lead the significant work of unifying IT and OT.

The convergence of IT and OT is crucial for modern industrial operations. Historically, IT has been the cornerstone of cybersecurity, focusing on data integrity, confidentiality, and availability in the corporate environment. However, IT professionals often lack a comprehensive understanding of OT networks and operations, which are integral in managing industrial control systems and physical processes.

Ultimately, a breach anywhere is a problem for everyone. That's why collaboration between IT and OT is essential. As digitalization evolves across industries and with respect to manufacturing, waves of new vulnerabilities are introduced. This expansion of the attack surface necessitates heightened vigilance to mitigate risks effectively.

STRATEGIES FOR EFFECTIVE OT SECURITY

A strong security position is a journey of continuous improvement. If you don't keep pace with the threat landscape, the cost could be determined by whoever holds you ransom. Whether a CISO or a team of IT and OT leaders are driving your security initiatives, there are several strategies you can implement to fortify your defenses.

Asset Inventory and Risk Assessment:

Maintain an accurate inventory of all OT assets. Conduct risk assessments to identify vulnerabilities and prioritize mitigation efforts. Assess each asset's criticality and allocate resources accordingly.

Modernize and Secure OT Architecture

Secure horizontal OT communication with standardized connectivity. Implement secure communication protocols across OT networks. Use consistent protocols that adhere to industry standards to ensure safe data exchange between devices, sensors, and control systems while minimizing vulnerabilities from disparate or outdated protocols.

Secure OT-IT integrations and vertical communications. Divide OT networks into segments based on function or criticality. Isolate critical assets from less critical ones to limit the impact of breaches. Segmentation prevents lateral movement by attackers and enhances overall security.

Implement Access Control and Authentication

Enforce strict access controls. Only authorized personnel should have access to OT systems. Implement multifactor authentication to prevent unauthorized entry. Regularly review and update access permissions.

Maintain System and Data Integrity

Keep up to date with software patches. Consider security requirements during OT installations and configurations. Leverage digital technologies for monitoring, predictive maintenance, and swift threat response.

Incident Response and Recovery

Develop robust incident response plans. Define roles, responsibilities, and communication channels. Regularly test incident scenarios and practice coordinated responses. Establish backup and recovery procedures to minimize downtime in case of an attack.

OT CYBER RESILIENCE & DIGITAL TRANSFORMATION THROUGH INDUSTRIAL CONNECTIVITY

Enterprise industrial connectivity bridges the gap between OT devices and systems and IT systems, enabling the seamless and secure movement of data from devices to OT and IT systems.

Enterprise industrial connectivity supports the modernization of IT-OT architectures, helping secure OT data while leveraging it to power digital transformation initiatives. Beyond robust device connectivity, it translates data from diverse OT assets into a standard (and compliant) format. To ensure OT data security, industrial connectivity solutions enable standardized, secure protocols, IT-OT network segmentation, and enforceable identity and access management (IAM) policies. These solutions fortify defenses with easily managed access control through standardized access and approval processes.

Industrial connectivity can also accelerate digital transformation initiatives through standardization. By standardizing on an interoperable solution, organizations can establish a consistent architecture across all their facilities. This enables companies to create playbooks—guidelines for responding to potential attacks—and mitigate cybercriminals' ability to infiltrate other systems or parts of the business.

Modernizing and standardizing data movement is critical to robust cybersecurity. Through industrial connectivity, users can minimize risks and ensure data integrity to boost their security posture and protect vital assets. Unlocking access to OT data enables performance management, predictive maintenance, and other digital transformation initiatives.

Data-driven insights empower teams at all levels, from optimizing production lines and managing supply chains to maintaining equipment. Scaling these practices across the enterprise leads to sustainable growth, competitive advantage, and better resource utilization—making industrial connectivity a palatable investment for all your business priorities.

Need more information? Learn More About PTC

21597 - Secure OT Networks through Industrial Connectivity Before Disaster Strikes