Trout

10 Steps to Protect Industrial Environments From Cyber Threats

21,000 industrial sites in Europe and North America face closure in five years due to rising cyberattacks, worsened by rapid tech integration and a cybersecurity skills shortage. This white paper offers a 10-Step Strategy to help industrial companies enhance cybersecurity and resilience.

Introduction

The scale of cyber threats targeting industrial systems has reached unprecedented levels. 39% of industrial organizations experienced a breach last year with 25% reporting losses between $1m and $10m. This trend is accelerating, with an 87% increase in incidents involving Industrial Control Systems (ICS) and Operational Technologies (OT) from 2021 to 2024. Forecasts predict that these attacks could shut down about 21,000 industrial sites in the next five years.

Sites can be secured in two ways: securing the endpoint and securing the network. Both approaches should be adopted. However, in industrial environments, enforcing endpoint security is challenging due to numerous third-party vendors and IoT devices. Therefore, securing the network carries more weight.

Traditional LAN setups are vulnerable to cyber threats and lateral movements from a connected workforce to core production machines. The air-gapped factory is becoming less common as more industrial organizations seek to adopt digitalization and leverage their data to increase efficiency and results.

Regulatory compliance adds another layer of complexity. Standards such as NIS2, ISO and NIST provide frameworks for securing industrial systems, but adhering to these regulations can be challenging.

In 2024, connectivity drives industrial performance. This whitepaper outlines ten steps to enable secure and rapid deployment of digital solutions in operations.

Industrial companies are left with a few core challenges:

- How can I build the foundation for a secure connectivity with limited resources ?
- Which stakeholders - internal and external - should be involved in these projects ?
- How can I prioritize efforts across topics and environments ?
- How can I accelerate and automate my environment compliance ?

The Current Landscape

In 2023, the cyber threat landscape remained relentless, impacting businesses of all sizes, from small and medium-sized enterprises (SMEs) to large corporations. Significant incidents include:

CHU de Brest (March 9, 2023):

A phishing campaign led to a serious cyberattack at CHU de Brest hospital. Hackers attempted to infiltrate the network and exfiltrate sensitive databases. However, due to the hospital's prompt response, the breach and system encryption were successfully averted. The disruption lasted two weeks, affecting vital operations like email communication, data sharing, and external database access.

DP World Australia Cyberattack (November 10, 2023):

DP World Australia, a pivotal port operator responsible for managing 40% of Australia's maritime freight, faced a severe cyberattack on November 10, 2023. This sophisticated cyber incident led to an immediate suspension of operations at key ports in Melbourne, Sydney, Brisbane, and Fremantle. Although incoming ships could unload, the attack hindered the outbound movement of freight, creating significant logistical challenges. The Australian government recognized the severity of the situation, describing it as "serious and ongoing", and actively coordinated a national response.

STEICO Group Cyberattack (March 1, 2023):

The STEICO Group, a leading German manufacturer of energy-efficient insulating materials, fell victim to a cyberattack, as disclosed on March 1, 2023. The breach, later detailed on their website, impacted both the production and administrative sectors of the company. A task force, including cybersecurity and data forensics experts, was immediately established to restore normal operations promptly. The specific nature of the attack, such as whether it was a ransomware extortion scheme, was not disclosed.

In parallel to these hacks and disruptions, legal frameworks have been introduced. Notably, the National Institute of Standards and Technology (NIST) in the United States has published NIST SP 800-82. This document provides comprehensive guidelines for securing Industrial Control Systems (ICS), which are vital components in critical infrastructures. Additionally, at the European Union level, the Network and Information Systems (NIS) Directive has been implemented.

This directive focuses on bolstering the cybersecurity of networks and information systems across the EU. It encompasses specific requirements for operators of essential services, a significant number of whom rely on ICS, thereby ensuring a more robust and standardized approach to cybersecurity in these critical sectors.

Trout

Contents

Step 1: Risk Assessment

To ensure the protection of industrial environments, it is crucial to start the process with a comprehensive risk assessment. This evaluation aims to identify the assets that could be impacted by a cyberattack, including hardware, systems, laptops, data, and intellectual property.As highlighted by NIST SP 800-82, conducting a risk assessment in the context of Industrial Control Systems (ICS) requires additional considerations that are not present when assessing the risks of a traditional IT system. Due to the potential impact of a cyber incident on an ICS, which can produce both physical and digital consequences, it is vital that the risk assessment incorporates these potential effects:

Impacts on safety and the use of safety assessments.
The physical impact of a cyber incident on an ICS, including its effect on the broader physical environment, the controlled process, and the physical effect on the ICS itself.
The implications for risk assessments of non-digital control components within an ICS.

This holistic approach ensures a comprehensive understanding of vulnerabilities and the necessary measures to enhance the resilience of industrials systems against cyber threats. We recommend using a simple matrix in these assessment like the one below.

Table 1

Impact / Probability	**Low**	**Medium**	**High**
Low		Guest Wifi	Employee personal devices
Medium	Physical security Systems (CCTV)	Point of sales Internal communication netwroks	Maintenance and operational systems ERP backup systems
High	Explosive warehouse ski lifts	Central sales systems	

What to do?

- Audit your physical site
- Fill the grid with your system and their risk evaluation
- Evaluate your coverage for each assets
- Set a reminder to review periodically

Step 2: Network Segmentation

To ensure the security of industrial environments, network segmentation is an essential step. *As defined by Tech Target, network segmentation is an architectural design that divides a network into multiple segments (subnets), each operating as a smaller, independent network. This effective strategy allows for the restriction of traffic in or to segments based on their location, as well as controlling where traffic can and cannot flow, including based on the type of traffic, its source, and destination. This approach is crucial for limiting the spread of a malicious attack, by confining the attack to a single segment.

To effectively implement network segmentation, it is recommended to follow the guidelines of the ISA/IEC 62443 standard which introduces the concepts of “zones” and “conduits”:

- Zone: consists of a grouping of cyber assets that share the same cybersecurity requirements.
- Conduit: consists of a grouping of cyber assets dedicated exclusively to communications, which also share the same cybersecurity requirements.

The standard requires that ICS networks should be segmented into zones based on criteria such as functionality, security level requirements, and risk to specific processes. This segmentation is key to isolating systems and assets with different security needs. It emphasizes the control of data flow between zones through conduits. Data flow should be restricted and monitored to ensure that only necessary and authorized communications occur between different zones. Each zone is assigned a security level (SL), and the standard provides guidance on the types of security controls to be implemented at each level. The segmentation should reflect these security levels, ensuring adequate protection for zones with higher security requirements.

What to do?

- Audit your network structure
- Validate of network segments are in place
- Validate that zones are grouping assets with the same requirements
- Define a process to add and remove assets from zones
- Set a reminder to review periodically

Step 3: Access Control

Network access control is a key aspect in enterprise environments, specially with the increasing interconnectivity required by modern business, ICS networks face heightened risks. This interconnectivity, including operations technicians accessing machines, vendor support, and the need for business data, breaks down the old isolation of ICS networks and opens up potential vulnerabilities to unwanted or malicious traffic. This situation highlights the necessity for strong access control measures.

NIST describes access controls as the process of managing requests for information and system access. The NIST SP 800-53 standard offers practical guidance on this. It includes policies and procedures for authorizing system resource usage, managing system accounts, and handling issues such as role separation, limiting user access only to necessary information (least privilege), and managing user sessions.

To simplify, imagine team members Alice and Bob in Team 2. According to these guidelines, they are authorized to access certain assets during specific times. This kind of clear, role-specific access management is what the NIST standard aims to achieve.

Furthermore, the CIS Controls document provides an easy-to-understand set of guidelines for Access Control Management. It acts as a useful benchmark for setting up and maintaining robust access control systems in an organization.

What to do?

- Audit your access control
- Validate what authentication systems are in places
- Validate if monitoring and alerts are in place for access controls
- Define a process to grant and remove access
- Set a reminder to review periodically

Step 4: Regular Software Updates and Patch Management

Regular software updates and patch management are fundamental for cybersecurity in industrial environments. Their primary function is to address security vulnerabilities and protect against emerging cyber threats. While these updates are crucial for maintaining system integrity and reliability, especially in industrial settings where failures can lead to significant disruptions, they also enhance overall system performance and ensure compatibility with new technologies.

Incorporating software updates and patch management into traditional IT processes is essential. This approach acknowledges the unique challenges in Operational Technology (OT) systems, such as difficulty in determining what elements to update due to vendor lock-in and the reliance on older operating systems no longer supported by vendors. Despite these challenges, integrating these practices into centralized IT processes ensures a more streamlined and effective management of cybersecurity risks.

Overall, a systematic, well-documented, and responsible approach to patch management in ICS environments is vital. This approach should be integrated into the organization's broader IT strategy, ensuring a comprehensive, secure, and efficient management of cybersecurity risks across all digital assets.

What to do?

- Establish a list of assets in your environment
- Validate for each asset that software updates and patches are received
- Define a process
- Plugged if possible in standard IT processes - to upgrade and patch
- Set a reminder to review periodically

Step 5: Employee Training and Awareness

Enhanced security stands as the primary motivator for businesses of all sizes to educate their employees, across all levels, about the importance of safeguarding against "human exploits" and cyber attacks. The ultimate objective of this training is to establish a robust human firewall capable of countering cyber threats. This is especially pertinent considering that, according to the Verizon 2021 Data Breach Investigations Report, 85% of data breaches in 2021 were attributed to the "human element."

To mitigate these risks, numerous compliance regulations, including HIPAA mandate cybersecurity training for all employees. Additionally, certain insurance requirements also stipulate the need for such training. This emphasizes that cybersecurity is not just a technical issue but also a human one, where informed and vigilant employees play a crucial role in maintaining the overall security posture of a company.

To enhance employees' knowledge in cybersecurity, non profit organization like such as The Global Cyber Alliance provide comprehensive training modules. These modules are accessible for most companies, from small to large. For instance, GCA has designed a unique kit for small and medium-sized businesses (SMBs), which encompasses crucial areas like software update protocols and business security measures, development of robust passwords coupled with two-factor authentication, and strategies to safeguard enterprise against phishing attacks.

What to do?

- Define a training and awareness plan, as well as tools, for your sites
- Identify “cyber champions” in each site to be the relay of your initiative
- Define channels for your employees to roll back questions and potential risk they see
- Set a reminder to review periodically

Trout

Step 6: Implementing Firewalls and IDS/IPS Systems

In Operational Technology (OT) settings, the implementation of IDS/IPS firewall systems is essential for enhancing network visibility, identifying threats, and ensuring resilient operations. These systems, designed to monitor and analyze network traffic, area great tool to secure industrial environments.

• Intrusion Detection Systems (IDS): These systems monitor network traffic and alert you if they detect suspicious activity or known threats. Think of IDS as a security camera, watching over your network and warning you of potential intruders.

• Intrusion Prevention Systems (IPS): These go a step further than IDS. Not only do they detect threats, but they also actively work to block them. IPS is like having a security guard who not only notices intruders but also stops them from entering.In terms of architecture, entreprise should break from a purely perimeter based approach to IDS/IPS and integrate these systems within different zones and conduit, as defined in the step 2.

Layer 5: Enterprise Zones

-Enterprise Network (Business and Logistics Systems)

-IDS/IPS for monitoring and protecting enterprise-level network traffic

Layer 4: Manufacturing Operations and Control

-Site Manufacturing Operations Systems (production scheduling etc)

-IDS/IPS for monitoring traffic to/from lower layers and enterprise layer

Layer 3.5: Demilitarized Zones (DMZ)

-Data Historian, Middleware

-IDS/IPS specifically for DMZ to monitor and control traffic between enterprise (Layer 4) & manufacturing zone (Layer 3)

Layer 3: Manufacturing Zone

-Supervisory Control Systems (SCADA, MES)

-IDS/IPS for monitoring internal manufacturing zone traffic

Layer 2: Area Supervisory Control

-Control Systems (PLC's, RTU's)

-IDS/IPS for monitoring communications to/from control systems

Layer 1: Basic Control

-Sensors, Actuators, Intelligent Devices

Layer 0: Process

-Physical Processes (Motors, Pumps. Valves)

What to do?

- Leverage your network structure identified in step 2
- Identify connections points between layers or zones
- Implement IDS / IPS systems at the connection points to monitor network behaviors
- Set a reminder to review periodically

Step 7: Data Encryption

Due to the often sensitive nature of the data processed by ICS, notably proprietary business data and personally identifiable information (PII), encryption is essential to preserve confidentiality and protect against intellectual property theft and privacy breaches in the event of cyber-attacks.

Yet, the integration of encryption within industrial environments is not without its challenges:

- Compatibility with Legacy Systems: A significant number of ICS components lack the capability to seamlessly integrate with modern encryption technologies. This mismatch poses a considerable challenge in retrofitting these systems with advanced encryption solutions.
- Complexity and Protocol Compatibility: The diverse nature of ICS components, often sourced from various vendors and built on different protocols, demands a sophisticated approach to ensure that the integration of encryption solutions does not impede system interoperability.

Addressing these challenges necessitates an agile approach to review “data flows”. Mapping these flows and which systems and conduits are involved will allow companies to validate if data is encrypted, at-rest and in-transit.

What to do?

- Map data flows in your industrial sites, with relevant tools associated to each steps
- Ensure encryption at rest is enforced in each systems
- Validate that encryption in transit is used for each conduit
- Set a reminder to review periodically

Step 8: Backup and Disaster Recovery Planning

In Operational Technology (OT) environments, the importance of robust backups and well-crafted disaster recovery plans cannot be overstated. Essential for maintaining system uptime and safeguarding data integrity, these strategies necessitate the regular creation of secure and accessible backups. Such backups should cover data and system configuration, enabling a rapid restoration in case of a cyber incident.

On the other hand, disaster recovery planning should, according to Tech Target, describe how an organization can quickly resume work after an unplanned incident. It involves identifying and prioritizing critical systems and processes, establishing clear roles and responsibilities for disaster response, and ensuring adequate resources are available for recovery efforts. This planning should also include regular testing and updating of the disaster recovery plan to ensure its effectiveness in the face of evolving threats and technological changes. It's crucial to have a clear communication plan in place to keep stakeholders informed during and after a disaster, thereby minimizing confusion and enabling a coordinated response.

This comprehensive approach, integrating both proactive recovery planning and a structured disaster recovery plan, ensures that all critical elements of incident management are effectively addressed. This strategy not only enhances the resilience of OT environments but also bolsters the capacity of the company to respond efficiently to incidents.

What to do?

- Ensure backup are in place for critical systems, both for their data and configurations
- Ensure encryption at rest is enforced in each backup
- Establish a disaster recovery plan mapping people, tools and processes
- Ensure Incident Response templates are in place for different segments - set a reminder to review periodically

Step 9: Continuous Monitoring

Continuous monitoring for OT and ICS systems is essential for maintaining resilient operations. Across the 8 steps mentioned above, controls should have been identified and if possible automated, to detect threats early.

Developing a continuous monitoring strategy aligned with the organization-level strategy involves (according to NIST 800-53) :

- Establishing and monitoring organization-defined system-level metrics.
- Setting frequencies for both monitoring and assessing control effectiveness.
- Conducting ongoing control assessments as per the continuous monitoring strategy.
- Ongoing analysis of system metrics and control assessment information.
- Responding to the outcomes of control assessments and monitoring.
- Reporting the system's security and privacy status to designated personnel at defined intervals.

In more practical terms, companies should be able to answer the following questions:

- What assets do I have and which ones are monitored ?
- How are my assets connected and are these conduit monitored ?
- What process do I have in place once an alert has been raised ?

We also recommend running regular pen testing exercice to ensure that systems are secured and automated detections are in place across assets.

What to do?

- Audit your physical site
- Fill the grid with your system and their risk evaluation
- Evaluate your coverage for each assets
- Set a reminder to review periodically

Step 9: Continuous Monitoring - Focus on pen testing exercise

🧠🔴 Red Team Pen Testing:

- This is like the offense in a game. The Red Team simulates the bad guys (hackers).
- Their goal is to attack and find weaknesses in the system, just like a real hacker would, but without causing real harm.
- They use all sorts of tactics and techniques to break into systems, find sensitive data, or disrupt operations, testing how well a system can withstand an attack.

🔵 Blue Team Pen Testing:

- The Blue Team is like the defense. They work to protect the system against attacks.
- Their job is to detect the attacks from the Red Team, respond to them, and strengthen the system's defenses.
- They analyze security systems, monitor network traffic, and investigate any signs of a breach to improve the organization's security posture.

🟣 Purple Team Pen Testing:

- The Purple Team is a mix of both offense and defense. It's not a separate team but a collaborative effort between the Red and Blue Teams.
- The purpose of the Purple Team is to ensure that the Red and Blue Teams learn from each other.
- The Red Team shares their attack methods and findings with the Blue Team, which then uses this information to improve defenses. This collaboration enhances overall security.

What to do?

- Audit your physical site
- Fill the grid with your system and their risk evaluation
- Evaluate your coverage for each assets
- Set a reminder to review periodically

Step 10: Regular Security Audits

In addition to intrusion detection systems, organizations must also have regular security audits in order to identify vulnerable processes before threats emerge. The goal of the periodic audit is to determine that the system is performing as intended, identify area of optimization and implement them. Monitoring efficacy and continuous optimization is among the pillars of most compliance frameworks, starting with ISO.

The results from each periodic audit should be expressed in the form of performance against a set of predefined and appropriate metrics to display security performance and security trends. Security performance metrics should be sent to the appropriate stakeholders, along with a view of security performance trends.

According to NIST SP 800-82, periodic audits of the ICS should be performed to validate the following items:

- The security controls present during system validation testing (e.g., factory acceptance testing and site acceptance testing) are still installed and operating correctly in the production system.
- The production system is free from security compromises and provides information on the nature and extent of compromises as feasible, should they occur.
- The management of change program is being rigorously followed with an audit trail of reviews and approvals for all changes.

What to do?

- Having implemented step 1 to 9 should have helped deliver on that step
- Define additional pillars you want to cover in your security policy
- Define controls for each pillars, and tie automated controls or reminder to them

Conclusion

In 2022, 57% of industrial organizations faced cyberattacks, with an 87% increase year over year in incidents involving industrial systems. To tackle this growing problem, we suggest ten simple steps:

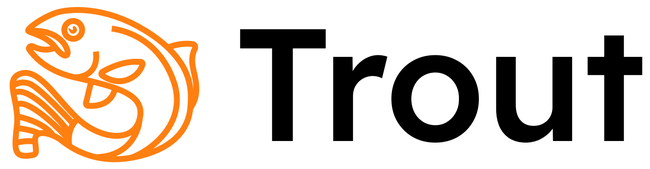
1. Risk Assessment: Identify and prioritize vulnerabilities.
2. Network Segmentation: Isolate systems to limit attack spread.
3. Access Control: Strictly manage who can access what.
4. Software Updates: Regularly update systems to fix vulnerabilities.
5. Employee Training: Educate staff to recognize and prevent attacks.
6. Firewalls and IDS/IPS: Deploy advanced systems for threat detection and prevention.
7. Regular Audits: Continuously assess and improve security measures.
8. Data Encryption: Protect sensitive data, both at rest and in transit.
9. Backup and Recovery: Ensure data integrity and operational continuity.
10. Continuous Monitoring: Vigilantly track and respond to threats.

By adopting this strategy, industrial entities can significantly reduce their cyber risk exposure, maintain operational integrity, and protect critical infrastructure against the growing sophistication of cyberattacks.

References

Detailed list of all regulations, frameworks, and standards previously cited:

-NIST SP 800-82
-NIS (Network and Information Systems)
-ISA/IEC 62443
-NIST SP 800-53
-CIS Controls
-HIPAA
-NIMS


Trout