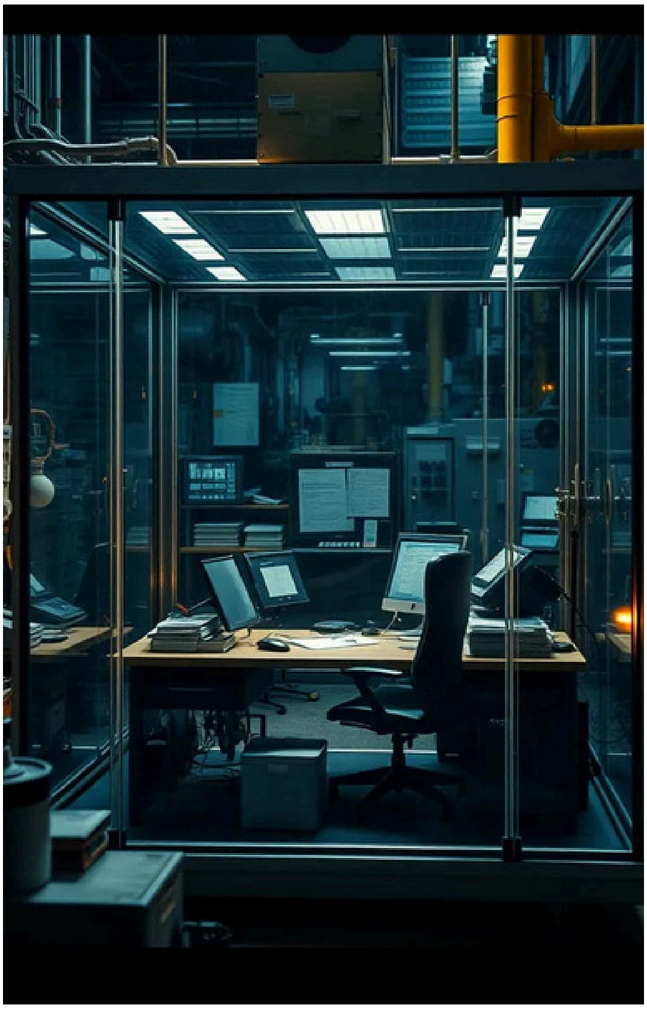
Why Cyber Attacks on OT Systems Are Escalating

Written by: Dr Michael Kelly, CISO of Cybernatics

03 April 2025

This white paper explores cybersecurity issues for OT-based organizations, such as manufacturing, energy and transportation companies.

Increasing threats from diverse actors using more sophisticated attack methods mean OT organizations need to be more concerned about how to protect their OT systems, especially since more of these are being connected to their IT systems and the Internet. Our experience with security projects for OT environments supports the need for these organizations to ensure they are concentrating on the SANS 5 critical sets of controls.

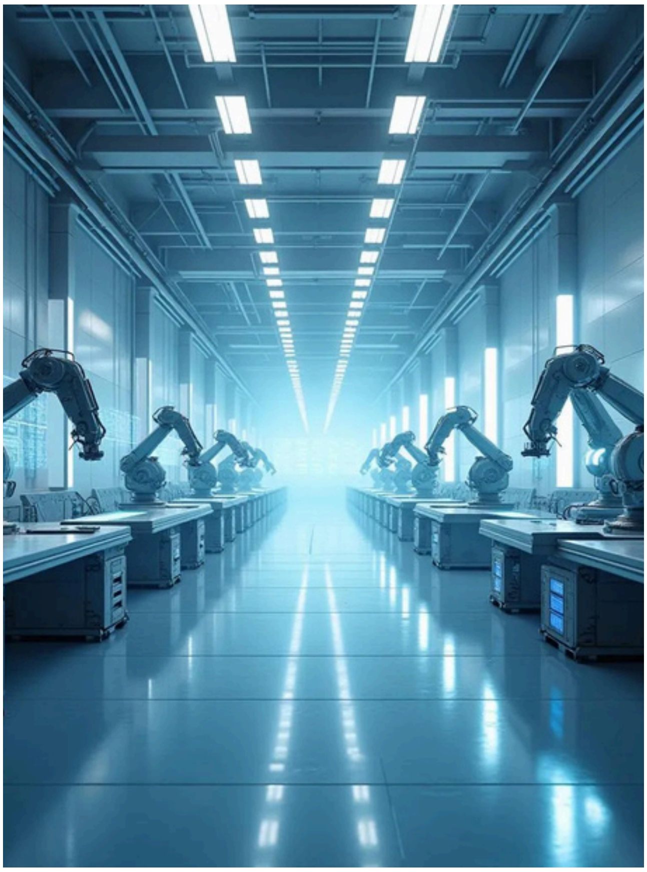


Operations technology (OT)

Operations Technology (OT) refers to the hardware and software systems used to monitor, manage, and control industrial operations. OT systems are critical in sectors such as manufacturing, energy, transportation, and utilities, where they enable the operation of physical processes. As OT systems become more interconnected with Information Technology (IT) networks, and even the Internet, they become increasingly vulnerable to cyber threats.

The impact of cyber-attacks on OT systems

Cyber-attacks on OT systems have increased substantially; Dragos reported that ransomware attacks on industrial organizations rose 87% in 2024 over 2023. Waterfall reported only a slight increase in the number of incidents that caused physical consequences, but increasing overall attacks. Successful cyber-attacks on OT environments can result in significant physical, financial, and reputational damage, making cybersecurity a critical concern.



Recent incidents exemplifying this point include:

- An attack on Peikko Group of Finland in December 2024 affected their ERP and 3D structural modelling software to halt manufacturing and deliveries, and to require manual operations for as long as 12 days.
- A sophisticated cyber-attack in September 2024 on Transport for London (TfL) compromised data on over 5,000 customers and caused the shutting down and restricting of access to systems to contain the damage, resulting in significant operational disruptions and £30 million in costs.
- Russian Internet provider Nodex was significantly disrupted in January 2025 by an attack on its infrastructure that required restoration from backup systems.

Because of the magnitude and increasing frequency of these attacks, government regulators have expanded their oversight and are emphasizing the need for robust cybersecurity measures, especially for critical infrastructure.

Key Cybersecurity Threats in OT

According to multiple sources, major cybersecurity threats to OT include:

- Legacy Systems with their own security vulnerabilities
- Increasing sophistication of attackers and their techniques
- Interconnections between OT and IT systems opening OT to attacks through IT
- Advanced Persistent Threats (APTs) targeting OT systems
- Ransomware attacks specifically to cause encryption of data for OT environments
- Exploitation of the broader attack surface from increased use of Cloud
- Nation-state actors targeting OT systems as part of broader geopolitical conflicts and cyber warfare strategies.

Key Directions for Enhancing OT Cybersecurity

To deal with these threats organizations are encouraged to apply foundation cybersecurity controls and principles to OT as well as IT, and then to concentrate even more on some key controls in the three key areas of technology, people and processes.

Strengthen Technological Foundations:

- Implement robust access controls and standardized security measures across the OT environments as well as the IT environments and their interconnection.
- Segment OT networks into smaller Zones of Trust to limit the spread of potential attacks.
- Enforce Zero-Trust remote access to OT assets, ensuring that all users are continuously authenticated and monitored.
- Implement solutions to monitor and alert in the OT environment
- Adopt AI and ML for threat detection and response

Develop Human Capabilities:

- Provide Specialized OT Cybersecurity training
- Encourage Information Sharing through OT Cybersecurity information sharing and Public-Private Partnerships to enhance OT cybersecurity knowledge and capabilities.

Improve Policies, Processes, and Governance:

- Establish comprehensive OT Cybersecurity policies and practices tailored to OT environments.
- Create and regularly update Incident Response and Recovery plans to ensure quick and effective action during cybersecurity incidents.
- Emphasize resilience to minimize the impact of cyber-attacks and ensure continued operation.

Implementing the SANS 5 Key Controls – What We've Seen

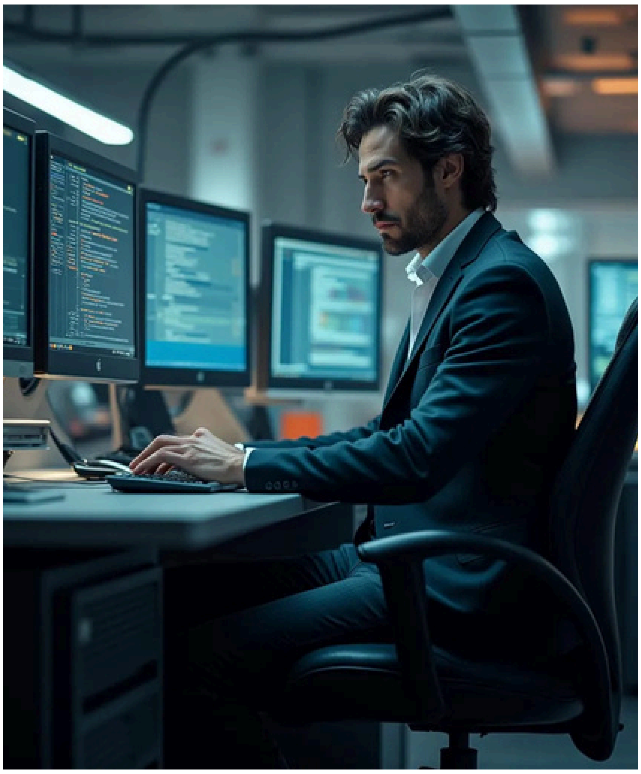
Implementing the SANS 5 Key Controls helps to enhance security in the areas mentioned above. The SANS 5 Key Controls for OT Cybersecurity address:

1. ICS Incident Response Plan
2. Defensible Architecture
3. ICS Network Visibility and Monitoring
4. Secure Remote Access
5. Risk-Based Vulnerability Management

We have been involved in a number of projects involving OT and IT security, and have found significant variation implementing these controls.

Manufacturing and critical infrastructure organizations can have complicated operating environments that make it difficult to compose an effective incident response plan. The emphasis on personal safety makes it difficult to integrate the cybersecurity incident response into the business incident response plan.

Having a defensible architecture generally requires an overall architecture that includes IT, OT and cybersecurity systems and operating principles. Organizations need to overcome the traditionally siloed understanding for these different areas, and pull together teams that can develop the overall plans. This combined defensible architecture is vital to design, implement and operate the last three topics.



Implementing a monitoring and alerting system for OT security is a major step for organizations that may still be struggling with IT security monitoring. Organizations need to determine whether to deploy separate solutions, such as the Cybernatics solution for OT security monitoring, or to integrate the log acquisition and monitoring within the IT Security Operations Center (SOC). In both cases organizations need to increase staff skills to understand cybersecurity related to both IT and OT operations.

To the extent possible, OT systems still need to be separated from external networks and the IT platform, even as the desire grows for greater data sharing from OT into IT and for IT generated controls into OT. External access controls need to be extremely strong, with mandatory zero trust. And protections against vulnerabilities and malware need to be maintained and operated in a manner that supports this network separation.

Conclusion

This white paper has examined the importance of cybersecurity for OT organizations because of increasing threats that can cause extensive physical, financial and reputational damage. To combat these threats requires use of technology, people and process controls. Implementing these controls in a manner consistent with the SANS 5 key control areas provides protection for OT organizations. Complications within OT organizations present challenges to implementing cybersecurity controls, challenges that companies such as Cybernatics are helping to overcome. Implementing the necessary cybersecurity controls is critical to running secure operations, resulting in better operational resilience.

[i] Dragos OT/ICS Cybersecurity Report, 8th Annual Year in Review 2025

[ii] 2025 OT Cyber Threat Report: Navigating the Future of OT Security, Waterfall and ICS Strive

[iii]Waterfall; and This white paper has examined the importance of cybersecurity for OT organizations because of increasing threats that can cause extensive physical, financial and reputational damage. To combat these threats requires use of technology, people and process controls. Implementing these controls in a manner consistent with the SANS 5 key control areas provides protection for OT organizations. Complications within OT organizations present challenges to implementing cybersecurity controls, challenges that companies such as Cybernatics are helping to overcome. Implementing the necessary cybersecurity controls is critical to running secure operations, resulting in better operational resilience.

[iv] Governments and industry regulators, such as the North American Electric Reliability Corporation (NERC) and the European Union Agency for Cybersecurity (ENISA)

[v] SANS Institute, MITRE, CiSA, Fortinet, Council on Foreign Relations, and others