ManuSec 2024

Cybersecurity Pulse Report

Navigating the Digital Frontier in Manufacturing:

Strategies, Challenges, and Innovations in Operational Technology Security for the Smart Factory Era

iSMG | #ManuSec

SPONSORED BY CyberEd.io

Table of Contents

Welcome & Overview

The latest edition of our Pulse Report series, the 2024 ManuSec.

Cybersecurity leaders, practitioners and marketing professionals require timely, actionable intelligence to combat emerging threats and leverage the latest innovations in operational technology (OT) security. This report, based on information provided by 61 industry experts and thought leaders from the 2024 #ManuSec USA Summit, delivers precisely that.

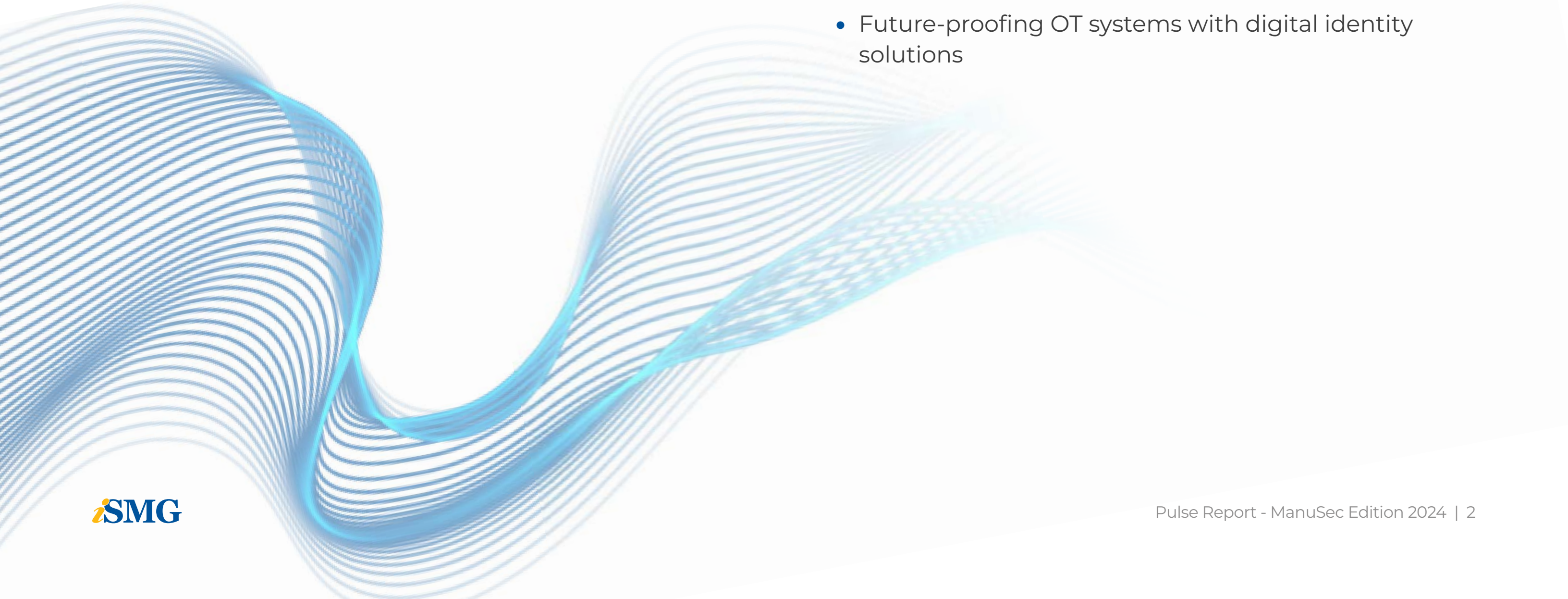
At ISMG, we are spearheading the use of advanced generative AI platforms and workflows to uncover detailed insights and bring them to you faster and in a concise and digestible format. This report exemplifies our commitment to leveraging leading-edge technology in service of cybersecurity knowledge sharing.

Our innovative AI-driven process has transformed more than 17 hours of video content from the 2024 #ManuSec USA Summit into this comprehensive report. This approach allows us to rapidly extract key insights from a vast amount of raw data, connecting cutting-edge research with practical application in record time. By harnessing the power of AI, we are able to identify trends, highlight critical information and consolidate diverse expert opinions into a cohesive narrative - all while maintaining the nuanced perspectives that make these conferences so valuable.

Our AI-powered workflow not only gets you the information faster, but it also enhances the quality and depth of our analysis, uncovering connections and patterns that traditional methods might miss.

The report covers critical areas shaping OT cybersecurity in manufacturing:

- IT-OT convergence and associated risks;
- Ransomware threats targeting manufacturing sectors;
- Shift from reactive to proactive security measures;
- Regulatory preparedness and compliance challenges;
- Strategies for communicating cybersecurity ROI to leadership;
- Vulnerability management in complex OT environments;
- Implementation of zero trust principles in OT;
- Data overload and alert fatigue management;
- Bridging the IT-OT divide through enhanced collaboration;
- Future-proofing OT systems with digital identity solutions



This report is essential reading for those at the forefront of OT cybersecurity. In our field, knowledge directly translates to improved security posture and preparedness. Whether you're a CISO developing security strategies for manufacturing environments, a practitioner enhancing your skills in OT security, or a marketing professional seeking to understand your audience's needs in the manufacturing sector, you'll find invaluable and unique perspectives here.

I encourage you to approach this report with an eye toward practical implementation. The ideas and innovations discussed are shaping OT security's future in manufacturing. The ideas and innovations discussed are actively shaping our industry's future. By leveraging this knowledge, we can collectively strengthen our defenses and build a more secure digital ecosystem.

Sincerely,

Daniel Verton

Dan Verton
Vice President, Content Intelligence and AI Innovation
ISMG

Introduction

As IT and OT systems began converging in the early 2000s, driven by the need for real-time monitoring, automation, and greater efficiency, the complexity of securing these environments increased. Traditionally siloed, IT managed data and communication, while OT handled physical processes on equipment that often was not designed with security in mind. Now, the blending of these two domains has created new vulnerabilities and requires a workforce that can seamlessly navigate both. This convergence highlights the critical need for specialized training to equip professionals with the skills to manage and secure these interconnected systems.

The skills required to navigate IT-OT convergence are far more nuanced than traditional cybersecurity roles. OT environments introduce unique vulnerabilities—often tied to legacy systems. Meanwhile, IT professionals are increasingly tasked with securing systems they aren't familiar with. Unfortunately, there's no standardized curriculum to fill this skills gap, and existing training often lacks the focus on the challenges inherent to IT-OT integration.

At CyberEd.io, we understand the educational gaps that exist in this space, and we're committed to closing them. Our platform offers tailored learning solutions that equip professionals with the tools they need to stay ahead in securing IT-OT environments. Whether you're a CISO, OT security engineer, or IT leader, continuous education is essential to thrive in this rapidly evolving landscape.

I invite you to explore this report with an eye toward your future. The cybersecurity challenges facing our industry are not static, and we cannot approach training as though static options are effective. The insights here are designed to inform, educate, and point you toward resources where you can apply what you've learned to safeguard critical infrastructure for years to come.

Stay safe, secure, and vigilant out there!

Brandy Harris

Dr. Brandy Harris
Director, CyberEd.io

Methodology

Our innovative approach transformed more than 17 hours of video content from the 2024 ManuSec USA Summit into this comprehensive report. Here's how we leveraged advanced AI technologies to distill key insights:

STEP 1 Content Processing

- Converted all video content from the summit sessions into accurate text transcripts.
- Cleaned and structured the raw transcripts to prepare them for analysis.

STEP 2 Thematic Organization

- Used AI-powered tools to automatically categorize content into key themes and subject areas relevant to OT security in manufacturing.
- Refined these categories and cross-referenced them to the key themes and topics of the ManuSec USA Summit Agenda.

STEP 3 Insight Extraction

- Employed advanced language processing to identify and extract critical insights, statistics, and expert opinions from the processed transcripts.
- Condensed lengthy discussions into concise, actionable takeaways.

STEP 4

Cross-Session Analysis

- Analyzed connections and patterns across different sessions and speakers to uncover overarching trends and common challenges.
- Identified areas of consensus and diverging viewpoints on key issues.

STEP 5

Report Composition

- Synthesized extracted insights into coherent, well-structured report sections.
- Refined language, ensured consistency, and optimized readability using AI-assisted editing tools.

STEP 6

Expert Review and Validation

- Our team of content marketing experts reviewed the AI-generated content, validating insights and providing additional context where necessary.
- Final human editing ensured the report's accuracy, relevance, and strategic value to our readers.

Securing OT and Manufacturing

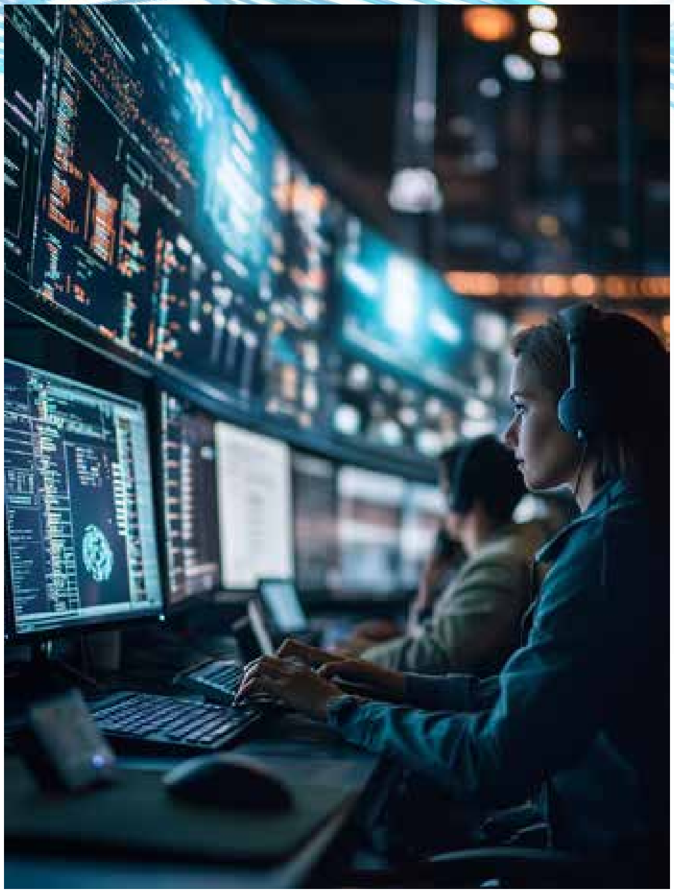
Overview of Operational Technology in Modern Manufacturing

Operational technology forms the backbone of modern manufacturing processes, encompassing the hardware and software systems that monitor and control physical devices, processes and events in industrial environments. As manufacturing becomes increasingly digitized and interconnected, the importance of OT in ensuring efficient, reliable and safe operations has grown exponentially. This evolution has necessitated a dual approach to security, balancing preventative measures with reactive capabilities.

The evolution of manufacturing into digitally connected smart factories has introduced both opportunities and challenges particularly in the domain of cybersecurity. As operations adopt advanced technologies such as Industrial Internet of Things (IIoT), artificial intelligence (AI) and cloud-based systems, scaling security strategies becomes critical to ensuring both innovation and operational resilience.

"OT cybersecurity is very much on the critical path throughout the whole asset life cycle ... from advisory and strategic planning right through to design, procurement and commissioning," said Chris Johnson, senior director, OT Cybersecurity and Digital Infrastructure at WSP.

Scaling security should incorporate a layered defense strategy, where multiple security controls are implemented at different levels of the manufacturing process. Real-time monitoring and behavioral anomaly detection should also be integrated to detect deviations in system behavior that may signal cyberthreats.



"Today ... there are two main types of controls: preventative controls and reactive controls," said Yair Attar, CTO and co-founder of OTORIO. "As you go more left of boom, it's more of a preventative control. On the right side, what we're seeing are more reactive detection-based solutions: intrusion detection systems, incident response technologies and SIEM solutions." This perspective highlights the dual nature of OT security, balancing proactive measures with reactive capabilities to protect critical manufacturing processes.

The integration of OT with information technology (IT) systems has led to significant advancements in manufacturing efficiency and capabilities. However, this convergence has also introduced new vulnerabilities and expanded the attack surface for potential cyberthreats.

“As OT environments became more complex, they needed to talk to backend servers on the IT side,” said Debbie Lay, principal solutions engineer at TXOne Networks. “But what ended up happening was opening up a new threat vector. You were now taking a traditional air gap and making it vulnerable.”

The Evolution of Cybersecurity Challenges in Manufacturing

The cybersecurity landscape in manufacturing has undergone a dramatic transformation in recent years. The convergence of IT and OT, coupled with the introduction of smart manufacturing technologies and the internet of things (IoT), has significantly increased the risk profile of manufacturing environments.

“More threat actors are targeting manufacturing because they know it’s a weaker link, and they’re willing to pay the ransom,” said Ebenezer Arumai, chief information security officer at Oldcastle BuildingEnvelope. This trend reflects the growing sophistication of cyber attacks targeting operational technology (OT) systems, where even brief disruptions can cause millions in losses - making manufacturers particularly vulnerable to ransomware demands.

The integration of legacy systems with modern, connected technologies presents a unique challenge in manufacturing environments. Many OT systems were not designed with cybersecurity in mind, as they were originally isolated from external networks. This legacy infrastructure, now exposed to new risks, requires careful handling to maintain operational integrity while enhancing security. The delicate balance between implementing necessary security measures and avoiding operational disruptions is a critical concern for industry leaders.

Innovation in manufacturing through smart technologies offers increased operational efficiency, predictive maintenance and reduced downtime. However, it also introduces new security risks as systems become more interconnected. Manufacturers must prioritize cybersecurity at the design stage of their smart factory transformations, integrating it into both new technologies and existing legacy systems.

“Resilience is a journey. There’s no destination … It’s a constant battle,” said Shane Williams, principal consultant - delivery, industrial cybersecurity at Black & Veatch.

Ensuring secure data exchange between cloud platforms, edge devices and factory control systems is vital.

“We need to make sure that we’re not messing with systems … at the end of the day, this is what makes the money,” said Rick Kaun, vice president solutions at Verve, a Rockwell Automation Company. He emphasized this point with a striking example: a pipeline company suffered a $17 million loss due to a mere two-minute reboot. This stark illustration underscores the high stakes involved in implementing security measures in OT environments, where even brief disruptions can result in staggering financial losses. It highlights the critical need for carefully calibrated security solutions that protect assets without compromising operational continuity.

The rise of ransomware attacks targeting manufacturing has become a pressing concern. These attacks can lead to prolonged operational disruptions and significant financial impacts. “We’ve seen ransomware impacting OT environments, even when not a targeted attack,” Lay said. Even after systems are restored, there are longer-term impacts on supply chains and business operations, she added, referring to the 2023 ransomware attack on Clorox.

The ransomware attack on Clorox disrupted its ordering and processing systems, leading to widespread product shortages and a substantial financial impact. Even months after the systems were restored, Clorox faced challenges in meeting consumer demand and reported ongoing effects on its supply chain and manufacturing capabilities.

Manufacturing organizations are shifting from reactive to proactive security approaches to address these evolving challenges. The complexity of securing modern manufacturing environments requires a strategic approach that considers both technological solutions and organizational processes.

“We need to establish aggressive, clear and measurable targets ... What does ‘done’ look like? What is the definition of an inventory?” Kaun said. This approach ensures that security efforts are focused and can demonstrate tangible progress to leadership.

The evolution of cybersecurity challenges in manufacturing reflects the industry’s broader digital transformation. As OT and IT systems become increasingly interconnected, manufacturers must adopt comprehensive, proactive security strategies that address their environments’ unique vulnerabilities while ensuring operational continuity.

While offering significant benefits, the integration of new technologies such as AI and IoT also introduces new risks that must be carefully managed. Moving forward, the manufacturing sector must balance the need for innovation and efficiency with robust cybersecurity measures to protect critical infrastructure and maintain operational resilience in the face of evolving threats.

Ransomware in manufacturing

Attacks on Manufactoring and Production Organizations (2020-2024)

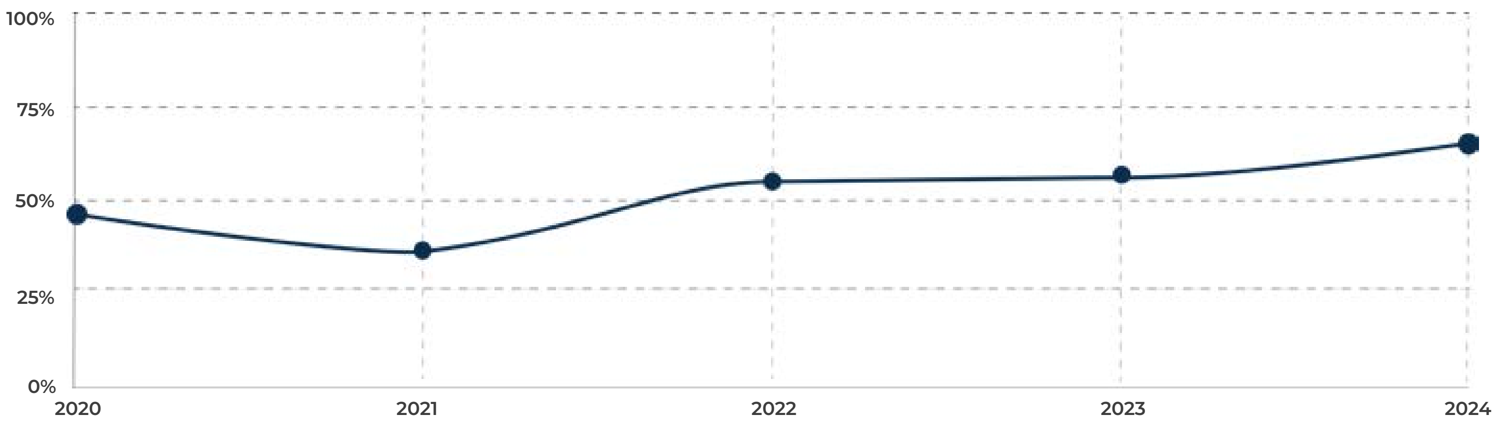


CHART 1. SOURCE: SOPHOS: THE STATE OF RANSOMWARE IN MANUFACTURING AND PRODUCTION

Strategic Security Approaches

From Reactive to Proactive OT Security

The cybersecurity landscape for OT is undergoing a radical transformation, marked by a decisive shift from reactive defense mechanisms to proactive, risk-based strategies. This paradigm shift is not merely a trend but a necessity for manufacturers aiming to safeguard their critical infrastructure against an increasingly sophisticated threat landscape.

A cornerstone of proactive OT security is comprehensive asset visibility and strategic vulnerability management. This approach goes beyond merely identifying assets; it emphasizes understanding the context and criticality of each component within the larger operational ecosystem.

Scaling security strategies to match the pace of digital transformation is a fundamental challenge. Manufacturing environments often include a mix of legacy systems alongside modern interconnected devices, making it essential to apply comprehensive security solutions that span both OT and IT. This should incorporate real-time monitoring and anomaly detection to provide continuous visibility.

“Context matters,” said Attar. “These assets belong to an oven within the assembly shop in an automotive manufacturing plant,” he said, as an example. “You need to have better visibility and understand the network configurations.”

This contextual understanding enables organizations to prioritize their security efforts more effectively, focusing resources on the most critical assets and potential points of failure. By gaining deeper insights into network configurations and the interdependencies of various systems, security teams can develop more targeted and efficient protection strategies, ultimately enhancing the overall resilience of their OT infrastructure.

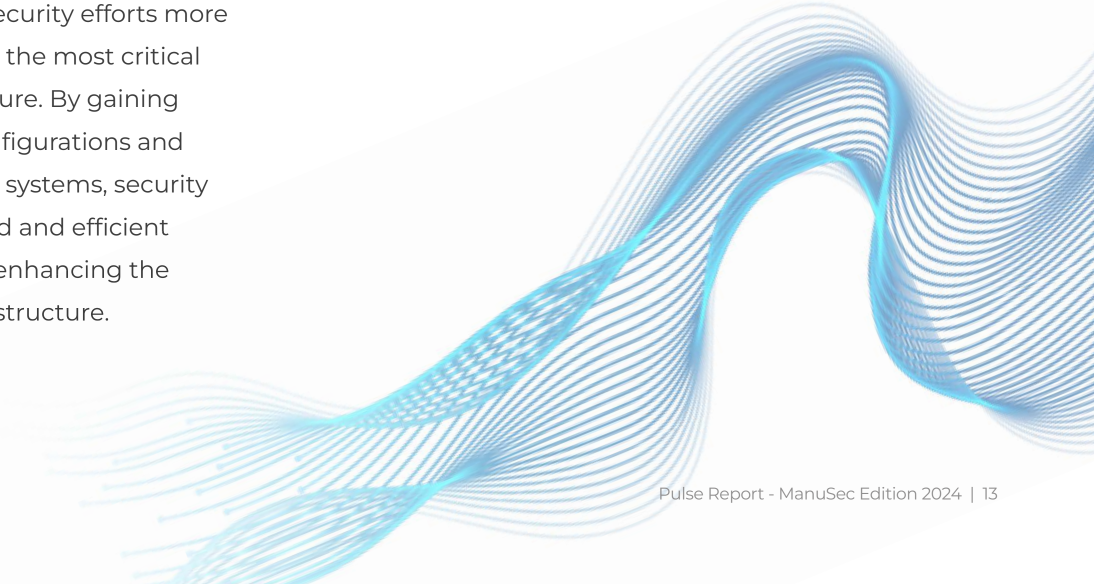
> “Context matters ... You need to have better visibility and understand the network configurations.”
>
> **Paul Gerste**
> Vulnerability Researcher at Sonar

Total Cost of Ownership and Cybersecurity Investments

When considering cybersecurity solutions, manufacturers must look beyond initial costs to understand the total cost of ownership (TCO). This includes factors such as scalability, deployment complexity and long-term maintenance. The true value of a security solution lies not just in its immediate capabilities but also in its ability to grow and adapt to the organization’s needs over time.

Attar cautioned against focusing solely on upfront expenses. He noted that while sensor-based approaches might seem attractive initially, they often fail to provide comprehensive coverage in large, multi-site environments.

Attar also stressed the importance of solutions that offer complete visibility and understanding across



complex manufacturing landscapes, even if they require higher initial investment. This perspective underscores the critical need for manufacturers to evaluate cybersecurity solutions holistically, considering long-term scalability and effectiveness alongside immediate costs. In the complex world of OT security, short-term savings can often lead to significant gaps in protection and higher costs down the line.

Regulatory Preparedness and Compliance

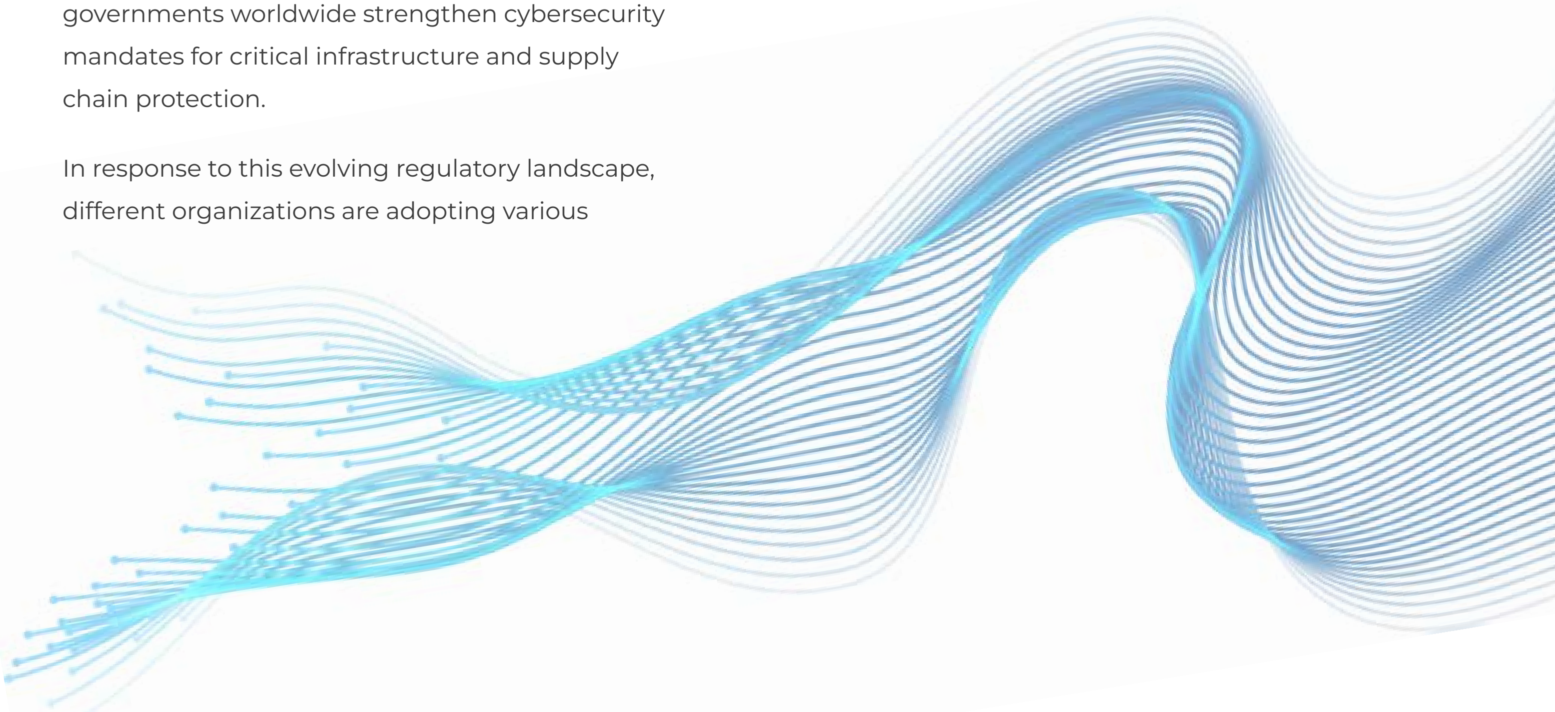
As regulatory scrutiny intensifies, manufacturers must prepare for compliance with various frameworks and standards. This proactive approach not only ensures legal compliance but also strengthens overall security posture.

“Manufacturing has traditionally been regulation light. But we’re anticipating changes,” said Scott Clayton, senior manager of manufacturing OT security and compliance at Lucid Motors. This shift signals a new era where manufacturers must balance operational efficiency with emerging compliance requirements, particularly as governments worldwide strengthen cybersecurity mandates for critical infrastructure and supply chain protection.

In response to this evolving regulatory landscape, different organizations are adopting various frameworks to build their compliance foundation. The choice of framework often depends on each organization’s specific needs and regulatory environment.

“We decided on the CIS framework mostly because it was very prescriptive,” said Joe Mariscal, director of cybersecurity and compliance at Ryerson. “As we’ve moved on … NIST comes into play, and we’ve used that to move into the DoD type space.” This evolution demonstrates how manufacturers are strategically layering security frameworks to expand market opportunities while strengthening their security posture - particularly when pursuing defense contracts and government partnerships.

Paul Wagner, director of IT-OT security at McCormick & Company, offered a different approach: “We beg, borrow and steal from the frameworks to come up with a model we can work with,” he said. “Adopting a framework in the absence of regulations, you can borrow the things that work for you.” This flexible approach allows companies to tailor their compliance strategies to specific needs and operational contexts.



Communicating OT Security ROI to Leadership

Effectively communicating the importance of OT security investments to C-suite executives is crucial for securing necessary resources and support. This often requires translating technical needs into business language that resonates with leadership.

Building a compelling business case for OT security investments involves highlighting the return on investment (ROI) in terms of avoiding costly downtime, regulatory penalties or the impact of a successful cyberattack.

For example, case studies of major manufacturing companies that suffered cyberattacks, such as the Triton malware attack, can be powerful in conveying the need for proactive measures. In the summer of 2017, Triton malware — also known as TRISIS and HatMan — was deployed against the safety controllers of a petrochemical facility in the Middle East. This marked a significant escalation in cyberthreats, as the attack specifically targeted

critical safety systems designed to prevent catastrophic failures. The malware's ability to manipulate these safety controllers underscored the growing risks to industrial facilities, where the consequences of a successful attack could result in extensive physical damage, system downtime and even the potential for loss of life.

"Once we were able to identify those types of catastrophic events … we didn't have to just talk toward the fear anymore. We had a real-life example of why we're trying to secure this environment, what the seven-figure investment was going to be necessary for," said Korey Wallace, manufacturing security lead at DuPont. This approach of using concrete examples helps bridge the gap between technical requirements and business impact.

However, calculating a direct ROI for OT security can be challenging, as the benefits are often in the form of risk avoidance rather than direct financial gain.

"We should stop talking about ROI when it comes to security," said Prasanna Ramakrishnan, CISO at Clarios. "The word we used at Clarios is, we said, it's the right thing to do, it's the responsible thing to do to secure our manufacturing facilities." This perspective shifts the conversation from ROI to risk mitigation and corporate responsibility.

Strategic security approaches in OT environments demand a proactive shift beyond reactive measures. Key to success are considerations such as total cost of ownership, adherence to regulatory compliance and effective communication of security priorities to leadership. By embracing these strategies, manufacturers can cultivate more resilient and secure OT infrastructures better equipped to confront the continuously evolving threat landscape.

> We should stop talking about ROI when it comes to security … it's the right thing to do, it's the responsible thing to do to secure our manufacturing facilities.
>
> **Prasanna Ramakrishnan**
> CISO, Clarios

Operationalizing OT Security

Developing Vulnerability and Patch Management Processes

Effective vulnerability and patch management is a cornerstone of OT security. However, with their mix of modern and legacy systems, the complexity of OT environments requires a thoughtful and often automated approach.

“We were ashamed of the vulnerabilities we had ... and we thought patching was the only thing we could do,” said Christian Harter, director of OT security and engineering at UPS. “We started understanding the reality that all software can be hacked, and operating systems can go end-of-life.” This realization led UPS to develop a more comprehensive approach to vulnerability management.

“We needed to do about $500,000 worth of fiber runs to try and actually do passive sniffing ... so we needed to find a different style of solution,” Harter said. “We ended up using CrowdStrike built on the Claroty platform.” Claroty provides visibility into operational technology (OT) networks by identifying assets, monitoring traffic, and detecting threats specific to industrial environments. Its platform allows organizations to secure OT and IoT systems by bridging the gap between cybersecurity and physical processes. By integrating with CrowdStrike, Claroty enables more efficient monitoring and protection of critical infrastructure without relying on extensive physical network modifications. This demonstrates the value of solutions that can scale and automate security in complex OT environments.

Christian Harter, Director of OT Security and Engineering, UPS.

Prioritizing critical vulnerabilities is essential, especially when dealing with legacy systems that can’t be easily patched. “We had some systems that were too old to patch,” Harter said, pointing to an example of a Windows 95 HVAC system connected to the network. “That popped up during a virus incident and required immediate action,” Harter said. This incident underscores a critical reality facing manufacturers: modernizing legacy OT infrastructure requires careful balance between security imperatives and operational continuity, often demanding innovative solutions beyond traditional patching.

Many legacy OT systems cannot afford downtime for security updates. Manufacturers can mitigate risks by adopting network segmentation techniques, where compromised systems can be

> “We were ashamed of the vulnerabilities we had... and we thought patching was the only thing we could do.”
>
> **Christian Harter**
> Director of OT Security and Engineering, UPS.

isolated without disrupting other critical operations. Real-time monitoring and automated scanning tools can also provide continuous visibility into the status of legacy systems, allowing for rapid identification and remediation of vulnerabilities.

UPS implemented a reporting system to track progress and maintain visibility. “We moved to Power BI for our reporting. We actually show how many vulnerabilities they have corrected, which made a big difference in how the team approached the problem,” Harter said. This approach not only helps manage vulnerabilities but also helps the security team to demonstrate progress to business leadership.

The Role of Governance in OT Cybersecurity

Effective governance in OT cybersecurity requires balancing centralized security standards with the flexibility to accommodate diverse operational environments. This is particularly important for organizations with multiple sites or global operations.

Experts acknowledged a clear need for a governance approach that includes standardized processes and tools. However, it must also be flexible enough to adapt to specific sites and regions. Each environment differs not only in architecture but also in people and processes.

Implementing a governance framework often involves collaboration between different teams within the organization. “We had to partner with our InfoSec folks,” Harter said. “They brought in a team that helped us - even though it didn’t feel helpful at the time, such as when they required an outside security assessment on our maturity.” This collaboration between OT and IT security teams is crucial for developing comprehensive governance strategies.

The governance approach should also consider the unique challenges of OT environments, such as the presence of legacy systems and the potential impact of security measures on operations. These challenges are often amplified by increasing regulatory demands, especially for organizations operating in or adjacent to critical sectors. Joe Mariscal’s experience at Ryerson illustrates this complex landscape.

“We’re critical-adjacent to the actual critical supply chain,” Mariscal said. “So, we have had companies that have sent us 300-question surveys. We might send them documentation or proof, but in general, the big controls are coming with CMMC,” he said, referring to the Cybersecurity Maturity Model Certification. This trend reflects how supply chain security requirements are cascading beyond primary contractors, forcing adjacent manufacturers to upgrade their security posture or risk losing valuable partnerships in the defense industrial base.

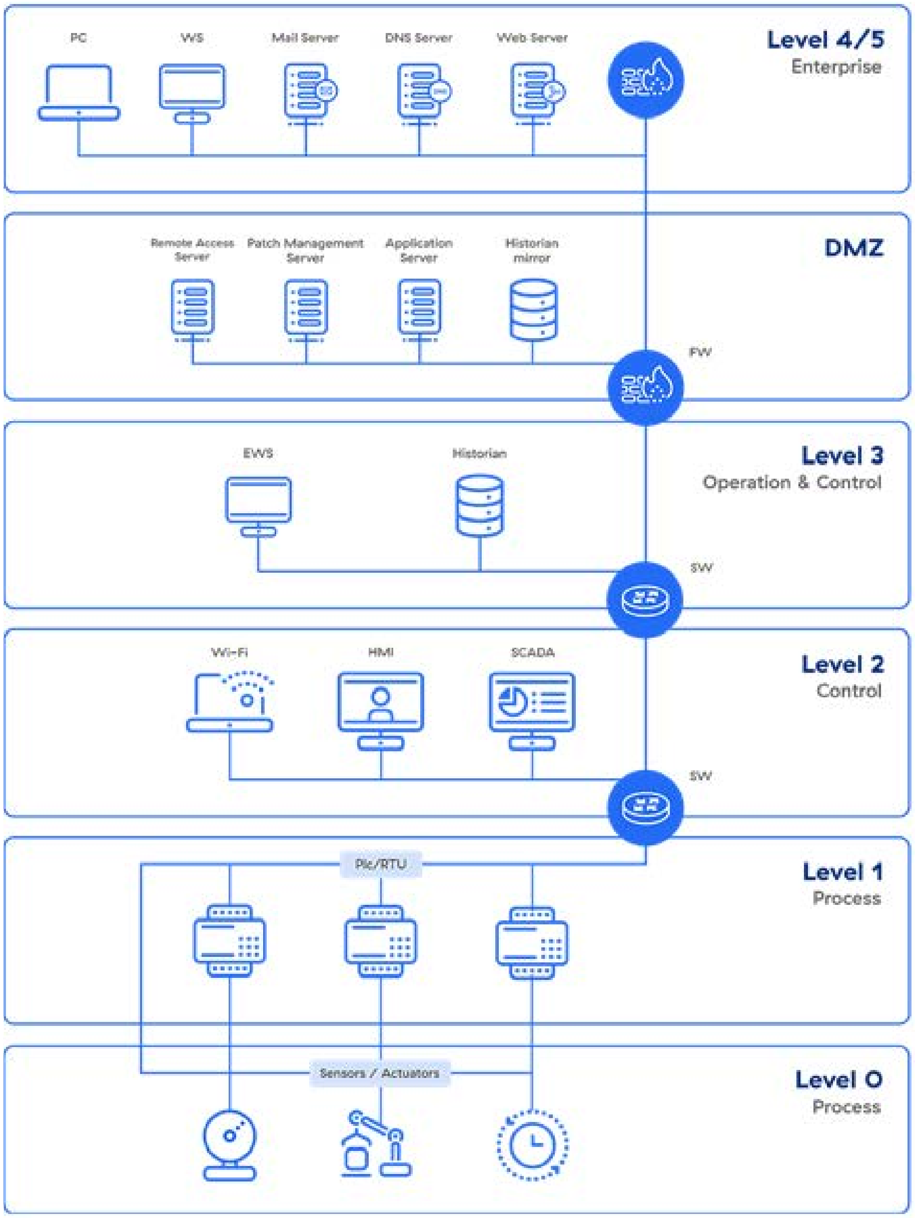
Operationalizing OT security requires a multi-faceted approach, including implementing structured security frameworks, developing robust vulnerability and patch management processes, and establishing effective governance strategies. By addressing these key areas, manufacturers can build more resilient and secure OT environments that are better equipped to face evolving cybersecurity challenges and regulatory requirements.

Detailed Concepts in OT Security

IT-OT Convergence and Associated Risks

The Purdue Model, traditionally used in industrial control system (ICS) environments, is a hierarchical framework that segments operations into distinct layers, from physical processes to enterprise-level IT. Each layer communicates only with adjacent layers, creating a clear separation between OT and IT systems.

However, with the rise of IoT and cloud computing, these boundaries are increasingly blurred. Devices in the lowest level of the Purdue Model, such as sensors and actuators (Layer 0), are now capable of communicating directly with cloud services, bypassing intermediate layers of control and security. This direct connection undermines the traditional segmentation and security zones the model relies on, as it introduces vulnerabilities and risks that can be exploited remotely.



Understanding OT/IT Convergence

The rise of IoT and cloud computing has eliminated the intermediate layers of control and security that traditionally separated OT from IT.

CHART: THE PURDUE MODEL FOR IT/OT SEPARATION, ALSO KNOWN AS THE PURDUE ENTERPRISE REFERENCE ARCHITECTURE (PERA), WAS ORIGINALLY DEVELOPED BY THEODORE J. WILLIAMS AT PURDUE UNIVERSITY.

As Ismail Guneydas, professor and chairman of the Cyber Security Program at Texas A&M University-Commerce, explains, this shift represents a major challenge for securing industrial systems. “With IoT and cloud computing, the clear-cut layers of the Purdue Model become blurry ... you have devices in Layer 0 talking directly to the cloud, bypassing traditional segmentation,” he said.

Supply chain vulnerabilities have increasingly emerged as a critical threat in the cybersecurity landscape, particularly within OT environments such as manufacturing. As supply chains become more digitized, the complexity of managing third-party access to OT systems grows exponentially.

“Even unintentional updates from trusted vendors can cause disruptions,” Lay said.

> “No longer do you have to broker [vendors] in their own Active Directory accounts. You don’t have to provision them VPN access where there’s an opportunity for lateral spreading on your network.”
>
> **Mike Bernard**
> Manufacturing Workflow Specialist, Imprivata

This highlights the need for robust supply chain security measures and careful management of third-party access to OT systems. Implementing a defense-in-depth strategy, which includes continuous monitoring, rigorous access controls and stringent supplier authentication mechanisms, is essential. Equally crucial is ensuring that third parties adhere to security best practices, such as providing secure patches and updates.

Zero Trust in OT Security

As traditional security perimeters blur in converged IT-OT environments, the concept of zero trust is gaining traction in OT security strategies. Zero trust principles, such as continuous verification and micro-segmentation, are being adapted to meet the unique needs of OT environments.

Mike Bernard, manufacturing workflow specialist at Imprivata, explained the importance of zero trust in OT. “Zero trust [is about giving] access only when needed and as granular as possible,” he said. “Use agentless solutions to avoid impacting OT devices.”

Bernard also elaborated on zero trust’s implementation in vendor access scenarios. “No longer do you have to broker them in their own Active Directory accounts. You don’t have to provision them VPN access where there’s an opportunity for lateral spreading on your network,” he said. “The concept is you can deliver through a temporary gateway directly into a particular asset — this could be a single smart thermostat, it could be into your PLC machines — it does not matter. The concept is that we want to challenge and enforce that their digital identity is delivered in a secure way to just those endpoints or just those assets and nothing else.”

This granular approach to access control is crucial in mitigating risks associated with third-party access in OT environments.

Asset Visibility and Access Control

Comprehensive asset visibility and effective access control are foundational to OT security. These elements are crucial for understanding the OT environment, managing vulnerabilities and implementing targeted security measures.

Ben C. Garber, lead solutions engineer at SCADAfence, emphasized the importance of asset visibility. “We have to know what’s out there, and we have to know its state in order to formulate a plan to effectively manage risk for those devices,” Garber said. This visibility challenge lies at the heart of OT security - where unidentified assets and unknown vulnerabilities can create critical business risks, particularly as manufacturing environments become more connected and digitally transformed.

Ralph Langner, founder and CEO of OTbase, highlighted the need for automated, real-time asset management. “If you’re still trying to do manual asset inventories, you’ve missed the train,” Langner said. “Today, your OT asset management system should tell you immediately which systems are affected by new vulnerabilities.” This real-time visibility is crucial for rapid response to emerging threats.

Langner also stressed the importance of contextual information in asset management. “You must have the capability to enrich basic information with context,” he said. “Geolocation, network association and physical process functions all need to be added by SMEs to make the data actionable.” This contextual understanding allows for more precise security management and decision-making.

Dynamic segmentation has become a crucial strategy for enhancing access control in modern cybersecurity frameworks. This method enables organizations to implement flexible, context-aware access controls that adapt to evolving operational requirements in real time. “When we’re bringing in vendors, we need dynamic segmentation to protect our environment,” said Ebenezer Arumai, chief information security officer at Oldcastle BuildingEnvelope.

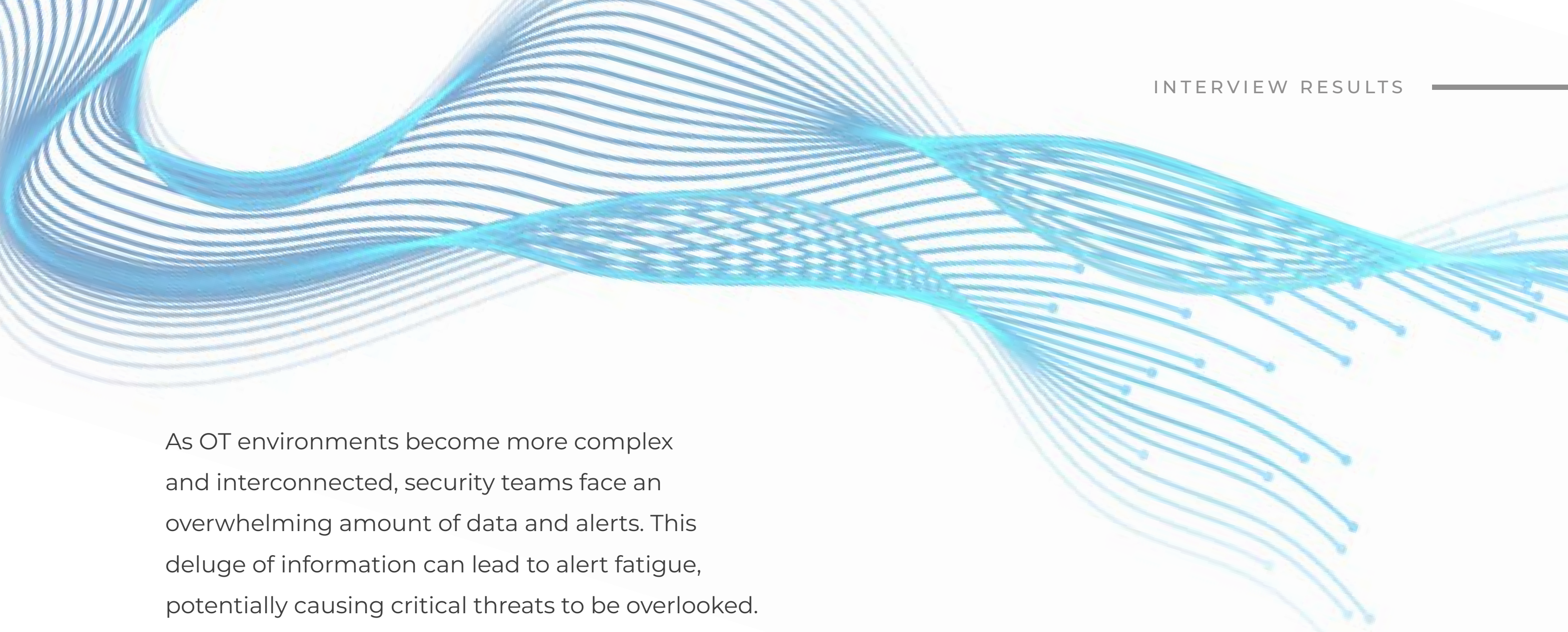
> “When we’re bringing in vendors, we need dynamic segmentation to protect our environment.”
>
> **Ebenezer Arumai**
> CISO, Oldcastle BuildingEnvelope

Addressing the challenges of IT-OT convergence, implementing zero trust principles, and ensuring comprehensive asset visibility and access control are critical components of a robust OT security strategy. By focusing on these key areas, organizations can strengthen their protection against evolving cyberthreats while preserving operational efficiency. Prioritizing these detailed security measures will help safeguard OT environments in an increasingly connected and vulnerable landscape.

> “We have to know what’s out there, and we have to know its state in order to formulate a plan to effectively manage risk for those devices.”
>
> **Ben C. Garber**
> Lead Solutions Engineer, SCADAfence

Data, Automation and Threat Prioritization

Managing Data Overload and Alert Fatigue



As OT environments become more complex and interconnected, security teams face an overwhelming amount of data and alerts. This deluge of information can lead to alert fatigue, potentially causing critical threats to be overlooked.

“Sixty percent say that they’re under alert fatigue. We have all of this data coming to a central location, and it’s fatiguing,” said Ben C. Garber, lead solutions engineer at SCADAfence. “There’s a lot of data to comb through, and how can we make sense of that?” This widespread challenge points to a critical need for intelligent automation and advanced analytics in OT security operations, where distinguishing genuine threats from noise directly impacts both security effectiveness and team productivity.

Organizations are turning to advanced tools and strategies that can filter and prioritize critical information to address this issue. Garber emphasized the importance of contextualizing data. “We prioritize exploitable vulnerabilities,” he said. “Start with the ones that have known active exploits. We need to be making these contextualized risk decisions.” This approach allows security teams to focus on the most pressing threats, reducing noise and improving response times.

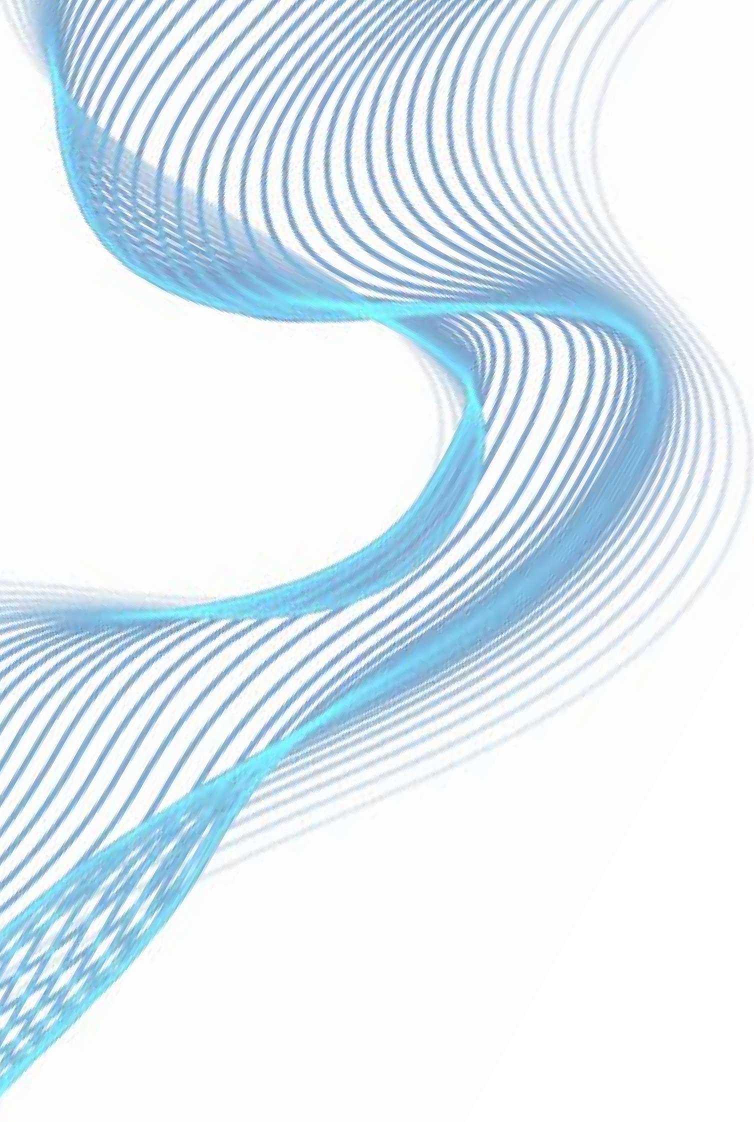
> DSPM can discover and classify, but they don’t do the difficult stuff.
>
> **Dubie Dubendorfer**
> Strategic Evangelist, Varonis

Automating Security Governance and Remediation

Automation is becoming increasingly crucial in managing the complexity of OT security. Automated tools can help organizations maintain consistent security postures across diverse environments and quickly identify and remediate vulnerabilities.

Dubie Dubendorfer, strategic evangelist at Varonis, emphasized the limitations of automation in security governance, noting that many data security posture management (DSPM) tools only handle surface-level tasks. “DSPM can discover and classify, but they don’t do the difficult stuff,” he said. “We need deeper analysis, monitoring, remediation and threat detection.” Dubendorfer’s insight underscores the need for more comprehensive automated solutions beyond basic discovery and classification. To effectively safeguard OT environments, organizations must adopt tools that can provide in-depth analysis, continuous monitoring and proactive threat detection, ensuring they address the more complex challenges of cybersecurity.

Automated remediation offers a powerful way to reduce the workload on security teams while improving response times. Dubendorfer explained that the goal is to both measure and maintain



security continuously. “If we had a beautiful image of all of our systems, we could track critical risks and dynamically adjust based on asset importance,” he said. This method allows organizations to maintain a proactive security posture, automatically addressing emerging vulnerabilities and ensuring critical assets receive the attention they need in real time.

Prioritizing Threats Based on Vulnerability and Exploitability

Not all vulnerabilities pose the same level of risk to an organization. Prioritizing threats based on their potential impact and exploitability is crucial for effective OT security management.

However, Langner cautioned against an overly reactive approach to threat management. “With the obsession about threats, most people working in OT security are just playing this Whack-a-Mole game, always chasing the latest threat or vulnerability, and that does not get you in a position to achieve improvement,” he said. Instead, Langner advocates for a more strategic, proactive approach to threat prioritization.

Managing data overload, utilizing automation for security governance and remediation, and prioritizing threats based on vulnerability and exploitability are essential components of modern OT security strategies. By adopting these approaches, organizations can better navigate the complex threat landscape of converged IT-OT environments, ensuring that resources are directed toward the most critical risks while maintaining operational efficiency. This proactive focus enables a more resilient and responsive security posture in an increasingly connected world.

> With the obsession about threats, most people working in OT security are just playing this Whack-a-Mole game, always chasing the latest threat or vulnerability.
>
> **Ralph Langner**
> Founder and CEO, OTbase

Bridging the IT-OT Divide

Enhancing Collaboration Between IT and OT Teams

The convergence of IT and OT has created a pressing need for enhanced collaboration between traditionally separate teams. This collaboration is crucial for developing comprehensive security strategies that address the unique challenges of both IT and OT environments.

“It’s challenging ... but plant walkthroughs with both IT and OT teams can bridge that gap, helping both sides understand what needs to be secured and how,” said Debbie Lay, principal solutions engineer at TXOne Networks. These joint walkthroughs offer a valuable opportunity for both teams to share knowledge, fostering a deeper understanding of each other’s responsibilities and security needs.

Lay recommended focusing on the right tools for the job to improve communication between IT and OT teams. “Make sure the security tools you choose are purpose-built for OT,” she said. “They must handle legacy assets and ensure fail-safe operation, even during upgrades or downtimes.” This advice highlights the need to select tools that meet the specific needs of OT environments and support smoother collaboration between IT and OT teams, helping bridge the gap in their differing requirements and approaches.

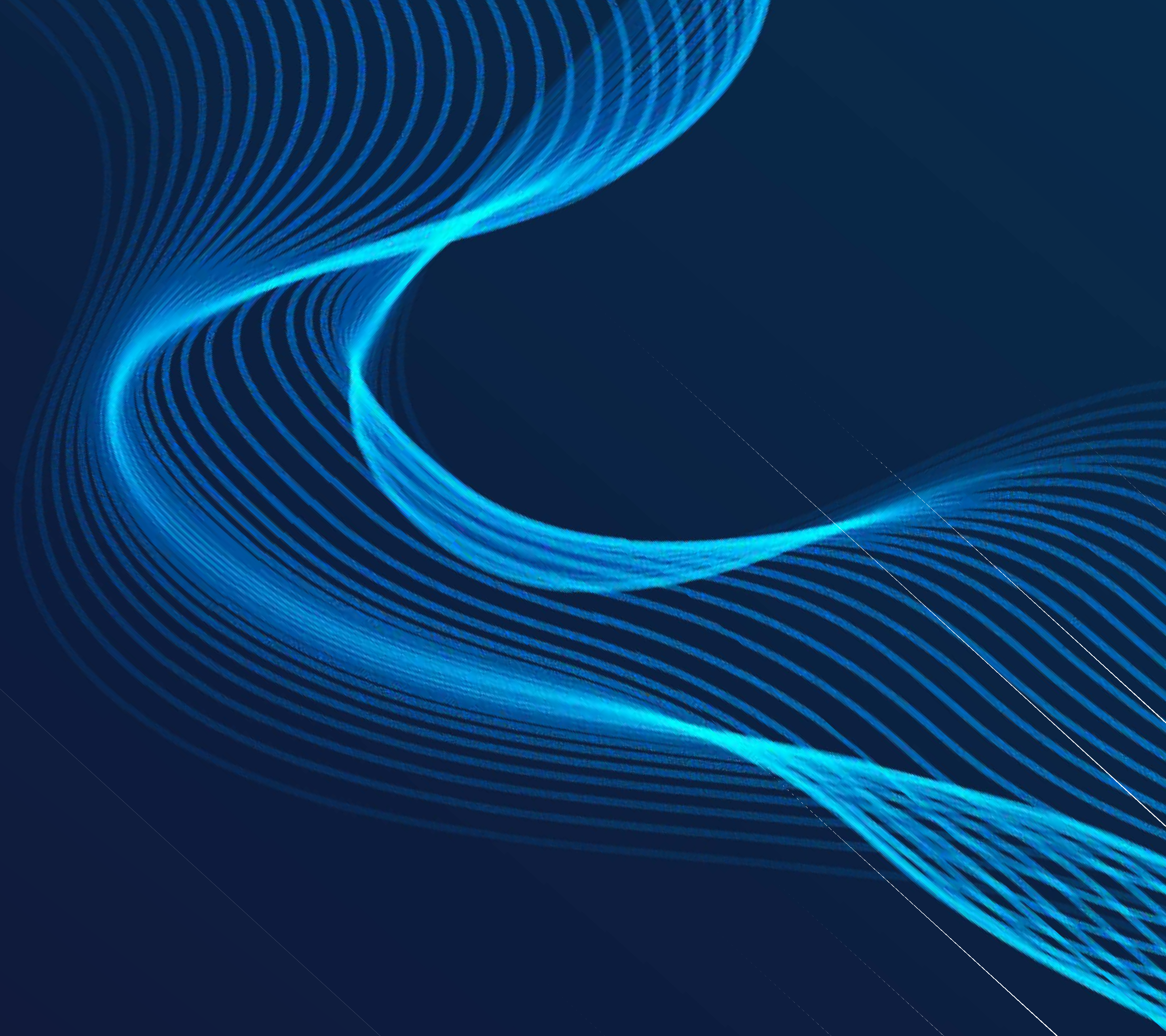
Building on this, Eduardo Giancristofaro, channel development director - OT at SSH Communications Security, highlighted the importance of implementing a zero trust model in OT environments. “Give access only when needed and as granular as possible”. he said. Together, these recommendations point to the necessity of security tools that not only bridge the IT-OT gap but also safeguard critical systems without disrupting operations.

Bridging the IT-OT divide requires a focused effort to foster team collaboration, leveraging joint activities such as plant walkthroughs and adopting shared, OT-specific tools. These initiatives allow IT and OT teams to better understand each other’s operational challenges and security needs, creating a foundation for stronger partnerships.

Additionally, managing third-party vendor access in OT environments is critical, as it introduces potential vulnerabilities. To mitigate this risk, organizations must implement stringent security measures such as granular access control, continuous verification and strict monitoring of third-party activities.

By addressing these challenges, organizations can build more resilient OT environments that integrate IT security best practices while meeting the distinct operational demands of OT systems. This balanced approach strengthens security and ensures operational continuity in increasingly interconnected infrastructures.

> Plant walkthroughs with both IT and OT teams can bridge that gap, helping both sides understand what needs to be secured and how.
>
> **Debbie Lay**
> Principal Solutions Engineer TXOne Networks



Looking Ahead: The Future of OT Security

The Role of Digital Identity in Future-Proofing OT Systems

As OT environments grow more complex and interconnected, digital identity has become vital for securing access across various systems and applications. This strategy enables a unified control plane to manage access in OT and IT settings.

Mike Bernard of Imprivata emphasized the importance of this approach. “Imprivata uses digital identity as kind of the core piece to making all of those things come whole,” he said. “Digital identity is like that broker to access. It’s what you touch in a digital world — all the data, all the applications, all the things that you guys deploy from an infrastructure perspective are what we want to be that gate to broker that access. So it doesn’t matter what type of applications you’re using; it doesn’t matter what type of hardware and endpoints we’re talking about here. Digital identity should be one control plane to access anything in your organization, both OT environments and on the production floor.” This holistic approach to digital identity management establishes a scalable and secure foundation for managing access in rapidly evolving OT landscapes.

Bernard further emphasized the need to balance security with user experience, stressing that organizations should not have to choose between the two. “No longer should you have to make that decision between security and end-user efficiency or productivity. Our mission is to deliver that, to give you that ability to not decide,” he said. “We want to be able to do that regardless of whether you’re a privileged user or a general frontline worker. The idea and the concept is that access should be controlled regardless of who you are and what you’re capable of accessing,” he said. This zero-trust approach marks a fundamental shift in OT security strategy, where granular access control becomes a business enabler - protecting critical systems while ensuring frontline workers maintain the access they need for operational efficiency.

Adopting Performance-Based Security

As OT security matures, there's a growing emphasis on performance-based approaches that focus on continuous improvement and measurable outcomes. This shift allows organizations to move beyond reactive security measures and demonstrate the ongoing value of their security investments.

Shane Williams, principal consultant - delivery, industrial cybersecurity at Black & Veatch, echoed the importance of this shift, emphasizing the role of communication in driving successful security changes. "If they understand the 'why,' they'll be much more amicable to accept the changes," Williams noted. "Without that, it's a failure." His insight supports the idea that aligning security improvements with clear, understandable goals is crucial for fostering buy-in and ensuring long-term success in OT environments.

Langner strongly supported the shift toward a performance-based approach to OT security. "You want to be in the promised land of performance-based OT security where you can measure and demonstrate your performance instead of always focusing on the latest threat or vulnerability," he said. This approach underscores the need to develop metrics that track security improvements over time, moving away from the constant cycle of reacting to emerging threats.

The future of OT security lies in leveraging digital identity as a core security component, preparing for emerging threats through clear, measurable objectives, and adopting performance-based security approaches. By embracing these forward-looking strategies, organizations can build more resilient, adaptable OT security programs capable of meeting the challenges of an increasingly complex and interconnected industrial landscape.

Contributors

List of Interviews Contributing to This Report

The following presenters participated in this year's #ManuSec USA Summit.

Khurram Anwar, CISO, CF Industries

Scott Avart, Director Global Information & Cyber Security, Archer Daniels Midland

Yair Attar, CTO and Co-Founder, OTORIO

Ebenezer Arumai, CISO, Oldcastle BuildingEnvelope

Mike Bernard, Manufacturing Workflow Specialist, Imprivata

Michael Bova, Senior Cyber Protection Advisor, Acronis

Scott Clayton, Senior Manager, Manufacturing OT Security and Compliance, Lucid Motors

Mark Cristiano, Senior Director, Global Solutions and GTM - OT, ServiceNow

John Dougherty, Head of Manufacturing, Americas, ServiceNow

Dubie Dubendorfer, Strategic Evangelist, Varonis

Daniel Eliot, Lead for Small Business Engagement - Applied Cybersecurity Division, NIST

Keatron Evans, VP, Portfolio Product Strategy, Infosec

Andrew Forgie, OT Cyber Specialist - North America, Armis

Laura Galante, Cyber Executive and Director of the Cyber Threat Intelligence Integration Center, Office of the Director of National Intelligence

Sean Galgay, Senior Solutions Engineer, RedSeal

Ben C. Garber, Lead Solutions Engineer, SCADAfence

Eduardo Giancristofaro, Channel Development Director - OT, SSH Communications Security

Ismail Guneydas, Professor and Chairman of Cyber Security Program, Texas A&M University-Commerce

Christian Harter, Director of OT Security and Engineering, UPS

Ward Holloway, Senior Director of Alliances, Bastille

Chris Johnson, Senior Director, OT Cybersecurity and Digital Infrastructure, WSP

Rick Kaun, VP Solutions, Verve, a Rockwell Automation Company

Tammy Klotz, CISO, Trinseo

Ken Koos, OT Security Engineer, Colgate

Kevin Kumpf, Chief OT/ICS Strategist, Cyolo

Ralph Langner, Founder and CEO, OTbase

Debbie Lay, Principal Solutions Engineer, TXOne Networks

Beth Letson, Global OT Cybersecurity Lead, Indorama Ventures PC

Jeramy LeMieux, VP, Environmental Health and Safety, Clarios

Jeffrey Macre, Industrial Security Solutions Architect, Darktrace

Joe Mariscal, Director of Cybersecurity and Compliance, Ryerson

Rafia Noor, Senior Manager - OT/ICS Cybersecurity, Colgate

Cathy Olsen, Director, Global Information Security, Packsize

Tim Oroszi, Principal Security Engineer, Tenable

Amit Pawar, Vice President, Consulting and Services, Xage Security

Chris Patteson, Field CISO, DeNexus

Deepak Patel, Senior Director, OT/IoT Security, Zscaler

J.D. Perham, Solutions Architect, Acronis

Daniel Peterman, US/Canada Controls Automation Manager, Clarios

Gary Phipps, VP of Strategy, ProcessUnity

Anthony (Tony) Pierce, Field CTO, Cyber Security and Infrastructure, Splunk

Vivek Ponnada, Technology Solutions Director, Nozomi Networks

Jorge Ramirez, Global Director of Manufacturing and Chief Manufacturing Cybersecurity Officer, GM

Prasanna Ramakrishnan, CISO, Clarios

Del Rodillas, Sr. Director of Product Management, Industrial Cybersecurity, Palo Alto Network

Steven Rosenthal, Director of Product Management, Critical Start

Jeff Rotberg, Strategic Partnerships Director, Tenable

David Ruzicka, OT Security Director, Clario

Douglas Santos, Director, Advanced Threat Intelligence - FortiGuard Labs, Fortine

Eric Schulz, CISO, Primient

KB Sharma, Executive Director, Head of Global Security Architecture, Engineering and Operations, The Estée Lauder Companies

Anup Singh, CISO, REV Group

Jenny Sissom, CISO, Allison Transmission

Paul Wagner, Director OT-IT Security, McCormick & Company

Korey Wallace, Manufacturing Security Lead, DuPont

Christopher Warner, Senior Security Consultant, GuidePoint Security

Friedrich (Fritz) Wetschnig, CISO, Flex

Shane Williams, Principal Consultant - Delivery, Industrial Cybersecurity, Black & Veatch

Andy Wilpizeski, Senior Solutions Architect, Dragos

James Winebrenner, CEO, Elisity

Chris Zimmerman, Director, Strategic Cyber Partnerships, Office of the Director of National Intelligence

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 · sales@ismg.io

BANK INFO SECURITY® · CAREERS INFO SECURITY® · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

CU INFO SECURITY® Just for Credit Unions · Data Breach® TODAY Prevention. Response. Notification. · infoRisk® TODAY · AIToday.io · CIO.inc

CyberEd.io · CyberEdBoard · DeviceSecurity.io · FraudToday.io · PaymentSecurity.io

CYBER THEORY · GREYHEAD AN ISMG COMPANY · Xtra mile LIFECYCLE MARKETING · QG MEDIA

iSMG