orange Business

orange Cyberdefense

NAVIGATING THE NEW INDUSTRIAL IT/OT SECURITY LANDSCAPE

ARC White Paper

July 2025

In today's industrial environment, cybersecurity is crucial for business resilience. The convergence of OT and IT, driven by the need for efficiency, increases connectivity and data-driven decision-making but also expands vulnerabilities. This integration exposes organizations to significant cyber threats, risking financial losses, reputational damage, and regulatory penalties..

By Thomas Menze
Senior Consultant,
ARC Advisory Group

ARC Advisory Group

VISION, EXPERIENCE, ANSWERS FOR INDUSTRY

CONTENT

Preface

This whitepaper is sponsored by Orange Business and Orange Cyberdefense, a leading provider of digital native services and networks services. Orange Cyberdefense specializes in threat detection, incident response, and managed security services, ensuring robust protection for industrial IT/OT systems. As cyber threats evolve, third-party cybersecurity services are increasingly vital for enhancing the resilience of industrial manufacturers. By leveraging expert solutions, organizations can safeguard their operations and focus on achieving their core objectives.

Executive Overview

In the context of modern industrial development, the integration of Information Technology (IT) and Operational Technology (OT) systems has emerged as a pivotal element in enhancing organizational resilience. A baseline level of cyber resilience is a prerequisite for the successful digital transformation of OT environments. Currently, the cybersecurity maturity of OT systems remains considerably lower than that of traditional IT infrastructures.

> *With the use of generative AI on the rise, cybersecurity services are vital for protecting industrial IT/OT systems. Partnering with trusted security consultants boosts resilience and lets organizations focus on core objectives, even without in-house experts.*
>
> *Thomas Menze*
> *Senior Consultant, ARC Advisory Group*

This IT-OT convergence, largely driven by the pursuit of operational efficiency, increased connectivity, and data-informed decision-making, offers substantial benefits in terms of productivity and process optimization. However, it simultaneously introduces a broader and more complex threat landscape. The amalgamation of these systems significantly increases the overall cyber-attack surface, thereby heightening the susceptibility of industrial control systems to malicious activities.

Adversaries exploit these expanded vulnerabilities, which may result in severe consequences, including operational disruptions, compromise of critical infrastructure, and threats to human safety. As such, robust cybersecurity strategies specifically tailored to the unique characteristics of OT environments are essential for mitigating these risks and ensuring the secure evolution of industrial digital ecosystems.

The advent of generative AI (Gen AI) further complicates the cybersecurity landscape. While Gen AI enhances threat detection and response capabilities, it also empowers malicious actors to launch sophisticated attacks. Industrial organizations face challenges in adopting cybersecurity solutions due to legacy system vulnerabilities, compliance requirements, and a shortage of skilled professionals. The gap between the need for qualified IT security experts and the available workforce continues to widen, leaving many organizations underprepared.

To navigate this new industrial IT/OT security landscape, organizations must prioritize resilience, adopt AI-driven defenses, and invest in comprehensive training and workforce development. Secure IT/OT integration is essential for optimizing processes, improving productivity, and meeting sustainability goals. Outsourcing cybersecurity services to specialized providers offers a pragmatic solution, enabling organizations to bolster their cyber resilience and focus on core operational goals.

Industrial Cyber Security: The Key to Business Resilience

In today's rapidly evolving industrial environment, industrial cyber security has become a foundational pillar of business resilience. The once-clear boundaries between operational technology (OT) and information technology (IT) are dissolving, driven by the need for greater efficiency, which in turn necessitates increased connectivity and data-driven decision-making. This integration, while offering significant operational advantages, also creates complex vulnerabilities that cybercriminals are increasingly eager—and able—to exploit.

Systems that were once isolated are now interconnected, meaning a breach in an IT network can rapidly cascade into production environments, disrupt operations, damaging critical infrastructure, and endangering human safety.

As IT and OT systems converge, the attack surface for industrial organizations expands dramatically. Systems that were once isolated are now interconnected, meaning a breach in an IT network can rapidly cascade into production environments, disrupt operations, damaging critical infrastructure, and endangering human safety. Business resilience, once measured in redundancy and disaster recovery protocols, must now account for the dynamic and persistent threat landscape that accompanies digitalization. Organizations that fail to recognize and address this shift risk significant financial losses, reputational damage, and regulatory penalties.

Impact of Generative AI

Compounding these risks is the advent of generative AI (Gen AI) technologies, which are both a boon and a bane for cybersecurity. On the one hand, Gen AI can empower defenders by enabling faster threat detection, automating responses, and improving system monitoring. On the other, these same technologies are being weaponized by malicious actors to launch highly sophisticated attacks. AI-supported systems can harvest personal information from social networks at an unprecedented scale and precision, crafting phishing emails and social engineering campaigns that are virtually indistinguishable from genuine communications. In this asymmetric battlefield, attackers can innovate faster than traditional defenses can adapt.

Cyber Security Services are an Established Market Segment with Outstanding Growth Rates

According to a 2024 ARC market study, the global industrial cybersecurity services market is projected to generate revenues of just over two billion dollars by 2025. This reflects an estimated year-on-year growth of nearly 20 percent.

Urgent Cybersecurity Challenges for Industrial Organizations

Market insights further highlight the urgency of the situation. Industrial organizations are increasingly aware of the growing cybersecurity threat but often struggle to keep pace with the complexity and volume of attacks. The adoption of cybersecurity solutions is rising, yet so are the challenges: from legacy system vulnerabilities and compliance requirements to the sheer shortage of skilled cybersecurity professionals. According to industry analyses, the gap between the need for qualified IT security experts and the available workforce continues to widen. This talent shortfall leaves many organizations underprepared, relying on outdated tools and overstretched personnel to defend against increasingly advanced threats.

The gap between the need for qualified IT security experts and the available workforce continues to widen, leaving many organizations underprepared and relying on outdated tools and overstretched personnel to defend against increasingly advanced threats.

In addition, the sophistication of modern cyberattacks is pushing traditional security models to their limits. No longer are attacks random or opportunistic; today’s threats are targeted, persistent, and potentially supported by nation-state-level resources. Industrial espionage, ransomware attacks on critical infrastructure, and supply chain vulnerabilities are no longer hypothetical risks but daily realities.

Converging Trends-IT/OT Integration

The converging of IT and OT in industrial cybersecurity must be understood in two dimensions. First, it reflects an industry-wide trend toward increased use of IT and IoT technologies to automate and optimize operational systems. Second, it introduces a new operational challenge within the Security Operations Center (SOC), where interdisciplinary collaboration between IT and OT security teams becomes essential to secure their growing interconnection. These converging developments—along with the disruptive potential of Gen AI, persistent barriers to cybersecurity adoption, and a shortage of skilled professionals—are fundamentally reshaping the industrial security landscape. To meet these challenges, organizations must rethink their cybersecurity strategies from the ground up, focusing on resilience, AI-enabled defense capabilities, and a cross-functional workforce. A consistent, unified security framework across all sites and regions is vital to ensure an agile, effective response. In an environment where digital risks increasingly have physical consequences, securing industrial systems is no longer just an IT concern—it is a core business priority.

Need for OT Security in Industry 4.0

The traditional separation between operational technology (OT) and information technology (IT) is dissolving as industries undergo IT/OT conversion to maintain competitiveness and enhance process efficiency. However, this transformation also opens the door for cyber criminals. The convergence of OT and IT introduces complex vulnerabilities, expanding the attack surface for cybercriminals. Industry 4.0 accelerates this risk, with connected systems increasing the severity of breaches. Attacks can disrupt operations, damage assets, and endanger safety. Many organizations lack the expertise to defend against these threats, and specialized OT security skills are scarce, requiring significant investment in training.

As a result, outsourcing industrial cyber security services is becoming a strategic imperative. Managed security services providers (MSSP) bring advanced threat detection capabilities, incident response expertise, and tailored security solutions that align with the unique needs of industrial environments. By partnering with specialists, organizations can rapidly bolster their cyber resilience, maintain compliance, and focus on core operational goals without overextending limited internal resources. Ignoring these trends risks operational disruption, financial loss, reputational damage, and regulatory penalties—outcomes no industrial enterprise can afford.

Business Resilience through Secure IT/OT Convergence

As previously stated, in today's industrial environment, cybersecurity is crucial for business resilience. The IT/OT convergence enhances efficiency but expands attack surfaces, exposing traditionally isolated systems to sophisticated cyber threats

Secure IT/OT integration is crucial for business resilience in 2025 and beyond. Through effective convergence, organizations gain greater visibility into their operations and can respond more dynamically to emerging cyber threats. Additionally, secure integration underpins digital transformation efforts, helping businesses optimize processes, improve productivity, and meet sustainability goals. However, this evolution also brings mounting regulatory expectations, demanding a mature and comprehensive security posture.

Addressing the Need for Specialized OT Cybersecurity Expertise in Industry 4.0

Without proactive investment in secure IT/OT convergence—whether internally or through trusted partners—organizations risk operational disruption, reputational harm, regulatory penalties, and the erosion of competitive advantage.

Challenging Areas to Increase Business Resilience

In the 2025 evolving industrial landscape, several cybersecurity trends demand urgent attention to protect operational resilience and ensure business continuity. **Visibility** is foundational for effective cybersecurity. You cannot protect what you do not know. In OT environments, where equipment and systems can last for decades, numerous undocumented changes and additions occur to address urgent business challenges. Without comprehensive visibility into all assets, networks, and system activities, organizations risk missing critical threats. Advanced monitoring tools and technologies provide real-time detection of anomalies, enabling swift and proactive responses to potential breaches. Visibility also supports system optimization and proactive maintenance, enhancing overall security resilience.

Digital transformation initiatives, such as the integration of Industrial Internet of Things (IIoT) devices, cloud platforms, and AI-driven analytics, offer significant operational benefits but also dramatically expand the attack surface. Every new digital touchpoint introduces vulnerabilities that, if unsecured, can be exploited by malicious actors. Industrial organizations must embed security into the core of their digital strategies, using encryption, access controls, and continuous assessments to safeguard their environments. Additionally, the evolution towards OT system virtualization, such as programmable logic controllers (PLC) in edge computing and local data centers, is a reality. This highlights that digital transformation is not solely a matter of cloud integration, which remains a challenge for many businesses, but also involves local compute solutions that align more closely with OT specificities.

Compliance is now a critical driver for cybersecurity investment. Regulatory frameworks such as **NIS 2, NIST standards, IEC 62443/21434,** and emerging **AI governance regulations** mandate stringent cybersecurity controls and practices. These standards are no longer optional; failure to comply can lead to substantial financial penalties, operational restrictions, reputational damage, and even legal action. Compliance is not just about meeting minimum requirements, it builds a culture of accountability, transparency, and trust with customers, partners, and regulators. Regular audits, adherence to best practices, and documented cybersecurity programs are essential to achieving and maintaining compliance.

Generative AI adds another layer of complexity. While AI can dramatically improve visibility and threat response, it also presents new risks, such as AI-generated attacks or misuse of autonomous decision-making systems. Establishing strong AI governance frameworks is critical to balance innovation with security and ethical use.

Given the growing complexity of managing visibility, digital risks, regulatory compliance, and AI governance, many industrial organizations face a significant skills gap.

Outsourcing cybersecurity services to experts offers a solution for several reasons. These experts bring the necessary technical depth, regulatory knowledge, and advanced tools to ensure organizations remain secure, compliant, and competitive. Compliance with regulations and directives is crucial, as these can differ significantly from region to region. Specialized providers are well-versed in the specific requirements of various regulatory frameworks, such as NIS 2, NIST standards, and IEC 62443/21434, ensuring that organizations meet all necessary standards and avoid substantial penalties.

In the era of AI, industrial automation systems face heightened risks from sophisticated cyber threats. Special measures to harden these systems include the deployment of AI-powered cybersecurity tools that analyze vast volumes of data in real-time, identifying subtle anomalies and detecting malicious activity. Zero trust architecture (ZTA) ensures continuous authentication and validation of every access request, minimizing the attack surface. Advanced endpoint detection and response (EDR) platforms offer behavioral analysis and AI-integrated threat prevention, helping to identify and contain threats before they compromise critical systems. Regular employee training and consistent patch management are also essential to maintaining robust security.

By outsourcing cybersecurity services, organizations can leverage these advanced methods and tools, ensure comprehensive protection while focus on their core mission in an increasingly complex digital and regulatory environment.

Key Industrial AI Trends in 2025

What are the key AI trends in industry this year? What percentage of AI is already being used in the IT and OT environment? A study by GlobalData on behave of Orange Business provides current answers to better assess these trends.

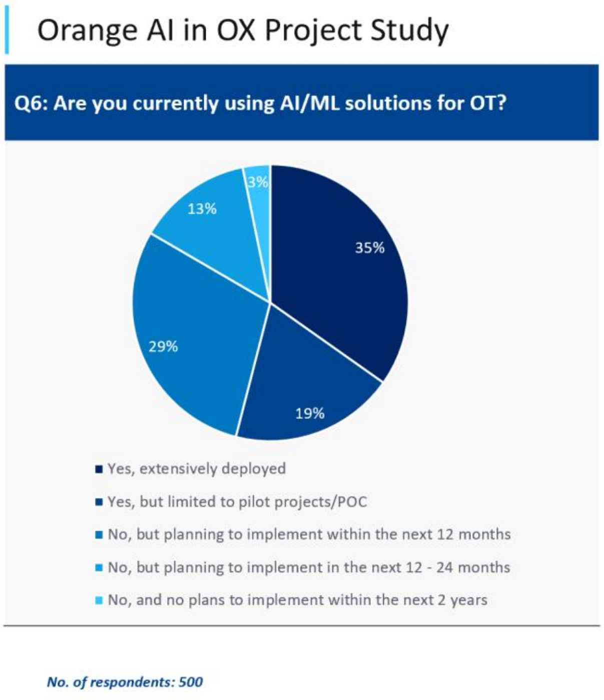
AI and Generative AI (GenAI) adoption in Operational Technology (OT) based on the survey results:

Widespread AI/ML Adoption:

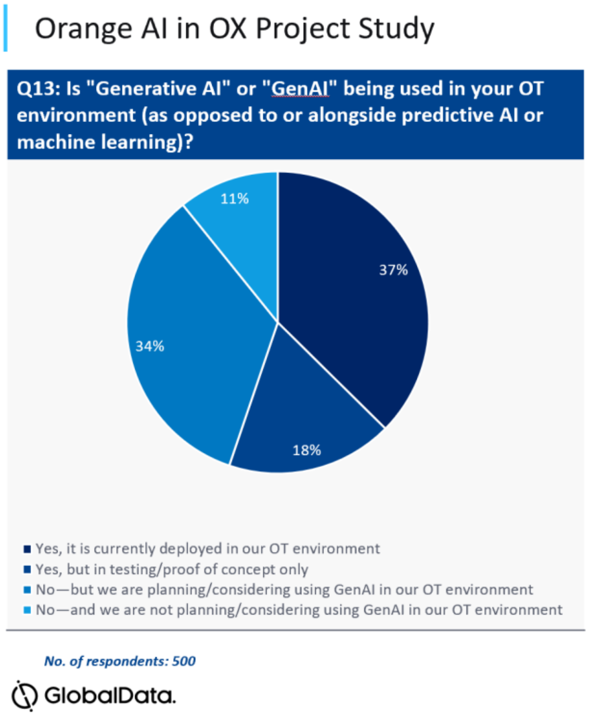
• A significant 97 percent of companies are either using, piloting, or planning to implement AI in their OT environments.

• Current AI use cases include predictive maintenance (53%) and condition-based monitoring (51%).

• Planned AI use cases for the next 1-5 years focus on employee effectiveness (65%), shipping documentation automation (62%), and demand forecasting (61%).



Status of AI in OT 2



Status of AI in OT 1

GenAI in OT:

• 37 percent of companies are already using GenAI, while 34 percent are planning to adopt it.

• Only 11 percent of companies are not considering GenAI.

• Industry leaders in GenAI adoption are steel/construction (51%) and pharmaceuticals (48%), while utilities (24%) and transport/logistics (26%) are slower adopters.

Infrastructure Challenges:

• Only 33 percent of companies believe their IT infrastructure is AI-ready.

- Key concerns include security (69%), cloud connectivity (51%), and legacy equipment (47%).

These trends highlight the growing importance of AI and GenAI in OT, with widespread adoption and significant planned use cases. However, infrastructure readiness and security concerns remain critical challenges for many companies.

What can be an AI-Generated Cyberattack?

AI-powered cyberattacks leverage AI or machine learning (ML) algorithms and techniques to automate, accelerate, or enhance various phases of a cyberattack. This includes identifying vulnerabilities, deploying campaigns along identified attack vectors, advancing attack paths, establishing backdoors within systems, exfiltrating or tampering with data, and interfering with system operations. AI-enabled cyberattacks can adapt to avoid detection or create a pattern of attack that a security system can't detect

One example is AI-driven social engineering attacks, where generative AI is used to create highly personalized and realistic emails, SMS messages, phone communication, or social media outreach to achieve a desired result. Another example is AI-generated malware, which refers to malicious software leveraging artificial intelligence techniques. Unlike traditional malware, these AI-enabled programs can autonomously adapt and improve, making them harder to detect

Securing Automation Against AI Cyber Threats

As AI becomes a double-edged sword in cybersecurity, industrial environments must proactively defend against increasingly sophisticated AI-generated malware. To remain resilient, industrial automation systems must evolve beyond traditional perimeter defenses.

A critical first step is the deployment of AI-powered cybersecurity tools. These systems excel at analyzing vast volumes of operational and security data in real time, identifying subtle anomalies, and detecting malicious activity that would evade conventional detection methods. By leveraging machine learning models, organizations can dynamically adapt to new threats.

Equally important is the adoption of zero trust architecture (ZTA). In an industrial setting, where lateral movement between systems can cause catastrophic disruption, ZTA ensures that every access request, whether from users, devices, or applications—is continuously authenticated and validated, minimizing the attack surface.

Modern endpoint protection is essential, with advanced EDR platforms offering behavioral analysis and AI-integrated threat prevention to identify and contain AI-generated threats before they compromise critical systems. However, modern EDR tools are optimized for IT environments and often do not support the older, proprietary operating systems or firmware found in industrial environments. Therefore, the preferred approach in industrial systems is to use network-based passive OT monitoring. Specialized OT security platforms leverage AI to provide threat detection based on communication and network behavior analysis.

Threat intelligence must be treated as a living resource. Staying updated on emerging AI-based attack tactics allows defenders to fine-tune their security posture and anticipate attacker behavior. In tandem, behavioral and anomaly detection systems offer a dynamic layer of defense by identifying deviations from normal industrial processes.

Human awareness remains a vital layer of defense. Regular employee training enables personnel to recognize suspicious behaviors or phishing tactics engineered by AI tools, significantly reducing the risk of user-enabled breaches.

Finally, consistent patch management is essential. Many AI-supported attacks exploit known vulnerabilities—regularly updating all software and firmware helps close these gaps before they can be weaponized. While consistent patch management is essential for closing known vulnerabilities and preventing AI-supported attacks, it presents unique challenges in industrial environments. These environments are highly sensitive and mission-critical, where even a short interruption or instability due to patch deployment can lead to significant production or safety risks. The interconnected nature of OT environments means that patches can have unforeseen consequences on dependent components or subsystems, potentially disrupting operations. Therefore, patch management in industrial settings requires careful planning, thorough testing, and coordination to ensure that updates do not compromise the stability and safety of the systems.

To safeguard modern industrial environments, organizations must adopt proven cybersecurity strategies that address both technical and organizational dimensions. First, comprehensive security services and consulting form the foundation of a proactive defense posture. This involves conducting in-depth risk assessments, customizing security architectures to industry-specific threats, and performing regular audits and penetration tests to uncover hidden vulnerabilities. Leveraging expert consulting ensures up-to-date alignment with evolving standards and threat landscapes.

Second, successful IT/OT integration strategies hinge on secure architecture and policy enforcement. Implementing strict access controls, encrypted data flows, and segmented networks helps isolate critical systems and prevent lateral movement by threat actors. Continuous monitoring and real-time incident response planning allow organizations to act swiftly under attack. Crucially, enabling close collaboration between IT and OT teams fosters operational cohesion and closes communication gaps that adversaries often exploit.

Third, a secure network infrastructure is essential to prevent both internal and external breaches. This includes deploying next-generation firewalls, intrusion detection and prevention systems, and maintaining a zero-trust model that authenticates every user and device. Routine network assessments and timely updates ensure that infrastructure remains resilient and aligned with best practices.

Finally, cross-functional collaboration and AI governance are increasingly vital. Establishing clear AI usage policies and cross-departmental workflows enhances organizational agility in threat detection. Training programs and awareness campaigns equip employees to recognize emerging threats. Implementing AI governance frameworks ensures transparency and accountability, minimizing the misuse of intelligent systems while maximizing their defensive potential.

Recommendations

As industrial environments become increasingly interconnected, the protection of operational technology (OT) systems from cyber threats has become a strategic priority. Industrial cybersecurity services play a critical role in securing industrial control systems (ICS), critical infrastructure, and complex networked environments. In summary, Orange Business together with Orange Cyberdefense — a leading managed security service provider (MSSP) — offers comprehensive services spanning all three core pillars of cybersecurity: Assessment, Design and Implementation, and Managed Services. For system operators, these services provide the structure and expertise required to safeguard OT networks in a rapidly evolving threat and regulatory landscape.

> *Effective cybersecurity in AI-driven operations safeguards critical assets, ensures compliance, and enables resilient, secure innovation through strong governance and alignment across IT, OT, and security teams.*
>
> *Emmanuel Routier,*
> *VP Operational Experience, Orange Business*

Assessment Services from Orange Cyberdefense allow operators to gain a clear view of their cybersecurity posture through asset identification, risk assessments, compliance audits (e.g., IEC 62443, NIS2), and penetration testing. These evaluations provide actionable insights into vulnerabilities and misconfigurations, enabling tailored remediation strategies that align with industrial needs and compliance demands.

Design and Implementation Services support the deployment of cybersecurity architectures purpose-built for OT environments. This includes network segmentation, secure remote access, and industrial-grade firewalls and IDS/IPS solutions. Orange Cyberdefense also assists in the creation of incident response plans, security policies, and targeted staff training. These services help maintain operational resilience while ensuring compliance with regulatory frameworks like the EU NIS2 Directive and the Cyber Resilience Act (CRA).

Managed Services offer long-term operational security by providing continuous monitoring, real-time threat detection and response, patch management, and integration of global threat intelligence — all supported by Orange Cyberdefense 24/7 Security Operations Centers (SOCs). This ensures that industrial environments are not only protected against emerging threats but can also react swiftly to incidents, minimizing downtime and risk exposure.

Importantly, these capabilities align closely with the findings of the ARC Champion Radar for Cybersecurity Services, which emphasizes that operators without in-house cybersecurity expertise face substantial challenges, especially as regulatory pressure intensifies. Since 2024, directives such as NIS2 and the CRA have raised the bar for incident reporting, risk management, and supply chain security. In this context, external providers like Orange Cyberdefense offer critical value by bridging technical and organizational gaps. Their services enable system operators to implement robust, compliant security strategies without overburdening internal resources.

In summary, Orange Business together with Orange Cyberdefense empowers system operators to secure their OT environments through expert-driven, end-to-end cybersecurity services that meet today's elevated regulatory and threat landscape.

Analyst: Thomas Menze
Editor: David Humphrey

Founded in 1986, ARC Advisory Group is the leading technology research and advisory firm for industry, infrastructure, and cities. ARC stands apart due to our in-depth coverage of information technologies (IT), operational technologies (OT), engineering technologies (ET), and associated business trends. Our analysts and consultants have the industry knowledge and first-hand experience to help our clients find the best answers to the complex business issues facing organizations today. We provide technology supplier clients with strategic market research and help end user clients develop appropriate adoption strategies and evaluate and select the best technology solutions for their needs.

This research has been sponsored in part by Orange Cyberdefense. However, the opinions expressed by ARC in this paper are based on ARC's independent analysis.

You can take advantage of ARC's extensive ongoing research plus the experience of our staff members through our Advisory Services. ARC's Advisory Services are specifically designed for executives responsible for developing strategies and directions for their organizations. For membership information, please call, write to, or visit our website:

ARC Advisory Group, Three Allied Drive, Dedham, MA 02026 USA • 781-471-1000 • www.arcweb.com