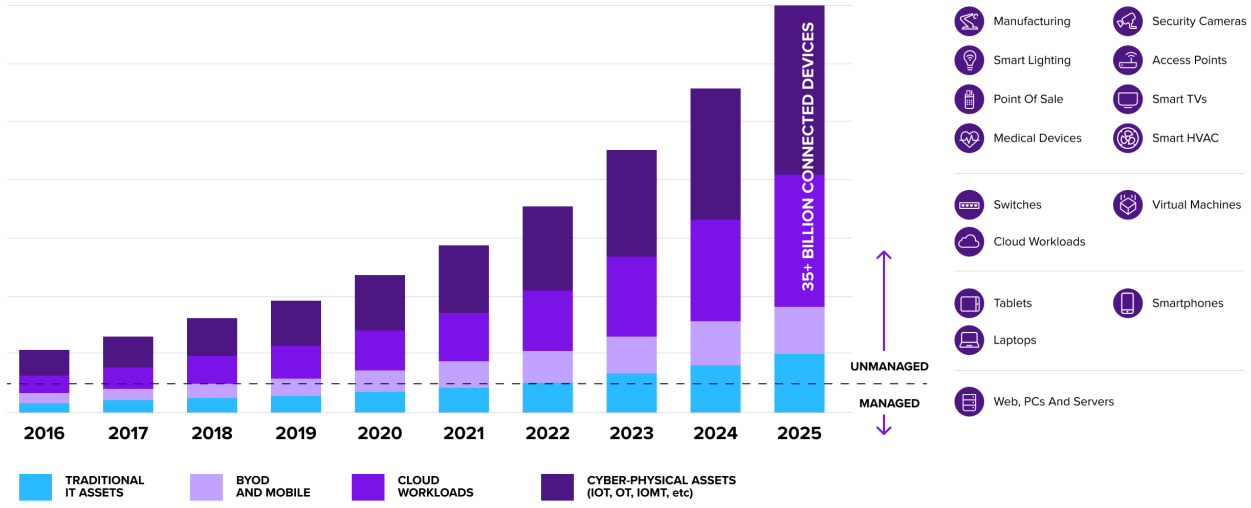
WHITE PAPER

Top 5 Emerging Security Priorities in OT and CPS Environments:

The Challenges We're Addressing Right Now

Overview

We're all familiar with the digital transformation sweeping through our critical industries, a trend that has been steadily gaining momentum over the past ten years. With devices and systems becoming more interconnected, cybersecurity risks and challenges are also growing in a similar trajectory. By the end of 2025, the number of connected assets is projected to reach a staggering 50 billion[1], highlighting the exponential increase in the attack surface for critical infrastructure. (In the figure below Armis highlights that a significant portion of these assets—up to 80%—may remain unseen, unmanaged, and lacking in security measures.)



For cybersecurity professionals, plant managers, OT specialists, and IT managers, staying ahead of these challenges is critical to protecting systems that keep our national infrastructure running smoothly- from water utilities and logistics networks to production lines and department stores. With the UK government pledging[2] to increase investment in AI, digitalization is unlikely to slow down and with that, a sea of new regulatory changes. With that in mind, here are our top trends shaping OT/CPS security right now.

[1] Armis Labs, 2024
[2] https://www.bbc.co.uk/news/articles/crr05jykzkxo

1. Cyber Exposure Management is the Response to a More Complex and Connected Attack Surface

The rapid digitization of industries has brought immense benefits, from automation to increased efficiency. Yet, every new device added to the network represents a potential entry point for cyberattacks. Cyber Exposure Management (CEM) is becoming critical in identifying, assessing, and mitigating these risks in an increasingly complex landscape.

Statistics to Consider

- Gartner predicts the IoT market will nearly double (including IIoT assets), soaring from $546 billion in 2022 to $991 billion by 2028.[3]
- 60% of organizations report that more than half of their industrial devices are not properly secured, making them vulnerable to attacks.[4]
- Industries are increasingly adopting sensors, actuators, and connected machines, but each new endpoint increases cybersecurity risks.
- Many IIoT devices come from third-party vendors, increasing the risk of supply chain attacks.

> *"The question isn't just about how many devices we can connect, but how we can secure these systems without stifling the innovation that drives it,"*
>
> **Michel Ruiz,** General Manager of Cyber Innovation at Honeywell Connected Enterprise.

Managing the Expanding OT Attack Surface

To tackle this challenge, organizations need proactive strategies that fall under the umbrella of Cyber Exposure Management, including early warning systems that can lift the curtain on attacker behavior left of boom, enhanced device inventory management, robust endpoint security measures, and network segmentation to limit exposure. Continuous risk assessment will be key to mitigating vulnerabilities across interconnected systems.

---

[3] Cybersecurity breaches survey 2024, UK Gov
[4] Armis Labs, 2024

2. Attacks are Moving From Monetary to Physical Harm

Enterprise IT systems and data are no longer the primary target for bad actors, as ransomware campaigns are now evolving to specifically target Operational Technology (OT) and Cyber Physical Systems (CPS). Major events like the BlackCat/ALPHV Ransomware attack, Salt Typhoon Telecom Hacks or CARR (Cyber Army Russia Reborn) Water Facility Attacks that have highlighted the need to have proper visibility across converged IT and OT environments .

And while ransomware has been around for almost two decades, its profitability potential has made it a go-to weapon for attackers. The rise of cryptocurrencies over the past five years has made it more difficult for law enforcement agencies to track digital payouts.

Attacks are evolving from immediate disruption (shutting down a plant) to compromising the integrity of industrial environments with intent to create physical harm. The potential costs of human life, litigation, insurance, regulatory fines, and reputation loss will be significant for organizations. Gartner[5] also predicts that most CEOs will be personally liable for such incidents. This is already playing out in the real world with notable examples including the SEC (Securities and Exchange Commission) charging a CISO for internal control failures.[6]

> *"Threat actors are continually seeking new ways to compromise systems, with the lower cyber maturity ICS and OT environments being squarely in their sights."*
>
> **Mirel Sehic,** VPGM Cybersecurity, Honeywell Building Technologies (HBT)

[5] gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024
[6] https://www.sec.gov/newsroom/press-releases/2023-227

3. A Magnifying Glass on OT and CPS Regulation

Governments worldwide continue to tighten cybersecurity regulations, with sector-specific directives expanding into critical industries like water supply, food and beverage, and pharmaceuticals.

Regulatory Updates expected in 2025

> **CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act)** in the U.S. is set to finalize and require critical infrastructure operators to report specific incidents to federal agencies. This will enhance threat detection and enable more rapid incident response.

> **Executive Order on Maritime Security** strengthens cybersecurity measures for port (sea) infrastructure and highlights the expanding scope of government initiatives to secure essential systems.

> **EPA Cybersecurity Mandates for Water Systems** aim to improve the protection of vital water infrastructure systems.

> **IEC 62443 Series (OT Security Standards):** Ongoing deadlines expected in 2025, global standard for securing Industrial Control Systems (ICS) and SCADA, focuses on risk management, incident response, and third-party security.

Globally, other regulatory frameworks such as the E.U.'s NIS2 Directive are setting stricter standards for OT security. These efforts promote resilience while fostering international collaboration to develop harmonized protocols for OT/CPS cybersecurity.

What Does This Mean for Security Teams?

It may seem obvious but organizations must proactively align their security approach with these evolving regulations. Preparing for audits, strengthening incident reporting capabilities, and building collaborative relationships with government agencies will remain top priorities.

4. Evolving Role of the CISO

The demands on Chief Information Security Officers (CISOs) are changing. They are increasingly expected to extend their influence beyond IT environments to address OT cybersecurity challenges.

The traditional role of the CISO is often insufficient for addressing the unique challenges of OT environments, where asset owners prioritize operational efficiency over traditional security concerns. To bridge this gap, there is a growing trend towards the emergence of specialized OT virtual CISOs or field OT CISOs. These professionals bring targeted expertise, helping to align cybersecurity leadership with the specific needs of operational technology.

Emerging Trends

- Board level priority, over 50%[7] of boards now consider cybersecurity a top priority, prompting CISOs to engage directly with senior leadership to align on risk mitigation strategies.
- Specialized OT CISOs and virtual CISOs are becoming common as companies recognize the unique complexities of OT environments.
- A recent Deloitte Global survey found that 20% of CISO roles now report directly to CEOs, up from 14% in 2023, reflecting the growing importance of cybersecurity leadership.[8]
- Regulatory pressures require CISOs to work more closely with CEOs and boards to manage cyber risk at a strategic level.

> *"Many businesses are moving through their own digitization journeys. This level of change will accelerate the convergence of IT and OT environments increasing the already large threat footprint."*
>
> **Mirel Sehic,** VPGM Cybersecurity, Honeywell Building Technologies (HBT)

[7] Gartner Cybersecurity Trends, 2024
[8] https://ceoworld.biz/2024/10/22/survey-reveals-growing-influence-of-cisos-as-strategic-leaders-in-business/

Strategic Focus Areas for CISOs

As the role of the CISO evolves, there are several key areas where CISOs are increasingly expected to focus:

01

Cross-Functional Collaboration:

As cybersecurity threats grow in complexity, CISOs must work closely with IT, OT, legal, risk management, and compliance teams to develop integrated, organization-wide cybersecurity strategies.

02

Crisis Management and Incident Response:

With the rise of cyberattacks targeting critical infrastructure and industrial systems, CISOs must have robust incident response plans that encompass both IT and OT systems.

03

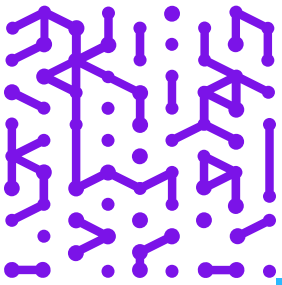
Building Cyber Resilience:

Beyond preventing breaches, CISOs are increasingly focused on building resilience within their organizations.

04

Board-Level Cybersecurity Attention:

With cybersecurity rising to the top of corporate agendas, CISOs must be able to communicate complex technical issues to non-technical board members and CEOs.



5. Government Level Investment in Artificial Intelligence (AI) and Machine Learning (ML)

Improving the security and resilience of OT and CPS systems is now one of CISA's top priorities, with an entire roadmap dedicated to how Artificial Intelligence can aid this.[9] Not a week goes by without a security bulletin delivered by their Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

AI and ML are transforming the way security teams detect and respond to potential threats. These tools are enabling faster, more efficient risk management by analyzing massive data sets in real-time for anomalies and potential vulnerabilities.

Applications of AI in OT Security

Early Warning System: Use AI to gain threat insights to foster a proactive approach to security posture.

Threat Detection: AI-powered systems can detect behavioral anomalies in OT environments that might otherwise go unnoticed, even if they mimic normal IT patterns.

Predictive Analytics: Advanced algorithms forecast potential risks and provide actionable insights before incidents occur.

Automation: Automating threat investigation and response allows teams to focus on higher-value tasks while minimizing disruptions to operations.

[9] https://www.cisa.gov/ai

Cybersecurity Priorities for 2025

Security teams are expected to focus on several overarching priorities to adapt to the evolving landscape. These include:

- **Zero Trust Architectures:** Implementing network segmentation and strict access controls across OT and IT systems.
- **Legacy System Modernization:** Upgrading or adding protective layers to aging infrastructure that may not meet today's security standards.
- **Unified Security Operations Centers (SOCs):** Consolidating IT and OT monitoring to gain holistic oversight of security threats.
- **Third Party Assets:** are increasingly targeted by cybercriminals. For 2025, a major priority will be ensuring the security of third-party relationships and the extended supply chain's software bill of materials (SBOM).
- **Cloud Security and Hybrid Environments:** With the increasing shift to cloud environments, particularly hybrid clouds that integrate both on-premise and cloud-based systems, cloud security remains a top priority

Looking Ahead

2025 is poised to be a pivotal year for OT and CPS cybersecurity. Governments and industries are ramping up regulations and standards, while organizations invest in technologies like AI and zero-trust strategies to stay ahead of sophisticated attacks.

Turning Challenges into Opportunities with Armis

At Armis, we believe that the convergence of IT and OT presents not only risks but also significant opportunities for innovation. By staying informed about emerging threats, regulatory changes, and technological advancements, organizations can leverage Armis' advanced cyber exposure management and security solutions to not only protect their critical infrastructure and ensure operational resiliency but also drive innovation.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial