



2026-2027

CYBERSECURITY REPORT

Cyber Intelligence from the Axians Frontline

By the Axians International
Cybersecurity Experts



Foreword

Cybersecurity now sits at the heart of business resilience. The threat landscape is evolving faster than many organizations can adapt, while the growing interconnection between technologies, operations and regulatory requirements is adding further complexity. Precise predictions remain difficult, but collective field experience can reveal recurring patterns and weak signals early enough for organizations to act.

Global reach, ground expertise

Every day, our customers share with us their challenges, priorities, transformation projects and cybersecurity concerns. Across industries, countries and levels of maturity, these experiences provide insight not only into evolving technologies, but also into the operational realities behind cybersecurity decisions. They reveal how organizations balance business objectives, regulatory requirements, operational constraints and resilience goals in an increasingly complex environment.

Intelligence built by practitioners

There are many cybersecurity reports, but this one offers another perspective: it is built by practitioners. Axians¹ teams design, implement, operate and secure digital infrastructures every day. We work with our customers before, during and after incidents, helping them strengthen resilience and make cybersecurity easier to manage. Axians also draws on the operational experience of Actemium, the industry brand of VINCI Energies.

This report's findings are grounded in customer engagements, delivery experience and lessons learned from real cybersecurity work. They capture critical customer pain points, core inquiries, and the patterns emerging across different industries and geographies. All examples have been anonymized, but the situations and insights behind them are real.

This intelligence was brought together by Axians' cybersecurity experts, SOC managers and analysts, Threat Intelligence specialists, pentesters, security architects, consultants and cybersecurity business leaders from across Axians. By comparing their observations, the report distinguishes isolated developments from the broader shifts organizations should already be addressing.



¹ Axians is the ICT brand of VINCI Energies, present in 36 countries through 385 business units and more than 16,000 employees.

From the lessons of 2026 to an action plan for 2027

Building on this collective intelligence, this report examines the developments that shaped cybersecurity in 2026 and the issues gaining momentum as organizations prepare for 2027. It translates field observations into practical actions across five areas:



Identity-centric attacks, ransomware, data theft and AI-assisted cybercrime continue to put organizations under pressure, making the ability to withstand and recover from disruption as important as prevention.

At the same time, governance, risk management and regulatory compliance are moving beyond the IT department to become enterprise-wide priorities. Protecting OT and critical infrastructure also requires security measures grounded in the realities of industrial operations.

AI is reshaping cybersecurity by creating new capabilities for defenders while exposing gaps in visibility and control, particularly around shadow AI and autonomous agents. Looking further ahead, quantum computing may remain a longer-term concern, but organizations already need to understand their cryptographic exposure and begin preparing for a post-quantum future.

This report is an invitation for you to prepare, not a prediction exercise. Its objective is simple: to help you anticipate, get ready and act.

Vincent Bazillio
Axians Cybersecurity Global Community Lead

Contents

The Threat Landscape

P.05

- 1.1 When every connection becomes a potential entry point p. 05
- 1.2 What changed on the cyber frontline in 2026 p. 06
- 1.3 Preparing for the next wave p. 08

Governance, Risk and Compliance: From Obligation to Operational Resilience

P.10

- 2.1 Regulation extends beyond the IT department p. 10
- 2.2 What 2026 revealed behind the compliance checklist p. 11
- 2.3 2027: Building governance for a broader risk landscape p. 13

OT Cybersecurity: From Operational Visibility to Board-Level Resilience

P.15

- 3.1 Visibility remains the foundation of OT cybersecurity p. 15
- 3.2 From technical controls to industrial resilience p. 16

The New Cyber Perimeter: AI, Identity and Control

P.22

- 4.1 Visibility lost, governance required p. 22
- 4.2 Securing the age of autonomous AI p. 24

Quantum Security Starts With Knowing What to Protect

P.26

- 5.1 Quantum in 2026: Simply curious, testing, or deploying? p. 27
- 5.2 Building quantum readiness before it's required p. 29

FINAL THOUGHTS

Building Resilience, Together

P.31

The Threat Landscape

1.1 When every connection becomes a potential entry point

The cyber threat landscape has become a fast-moving environment in which identity theft, phishing, ransomware, data exfiltration and AI-assisted attacks increasingly overlap. Among Axians' customers' engagements and operational security activities, one reality stands out: attackers are becoming faster, more targeted and increasingly able to industrialize their operations.

For many years, organizations focused mainly on protecting infrastructure. Today, **digital identity** has become one of the most valuable attack surfaces. Account compromise remains one of the most frequent incidents encountered in day-to-day operations, despite progress in awareness, endpoint protection and access control. In parallel, attackers exploit Internet-facing vulnerabilities more aggressively, at least within days of disclosure and even less time. With AI, this window may shrink further, turning remediation into a race measured in minutes or seconds².

Artificial intelligence is adding another layer of complexity. At Axians, we see AI as both a risk and an opportunity. It is changing the scale and efficiency of cyberattacks: language barriers, poor grammar, and unrealistic scenarios are no longer reliable warning signs in phishing. AI now enables attackers to create convincing messages, professional-looking content and targeted fraud attempts at unprecedented speed.

The result is a threat landscape where trust itself has become a target. Every email, identity, supplier relationship and digital interaction must now be verified rather than assumed legitimate.



AI will be the main driver of Cybersecurity change in 2026

Security leaders expect AI to reshape both attack and defense

Source: World Economic Forum, Global Cybersecurity Outlook 2026

² For more on AI in cybersecurity, see page 22.

1.2 What changed on the cyber frontline in 2026



"The most frequent incidents we investigate are no longer sophisticated intrusions but account compromises. Even with awareness programs and training, identities remain the primary target because once an attacker gains access to a legitimate account, they can operate through trusted channels and conduct highly credible fraud attempts."

Loubna Izika
SOC Manager, Axians France

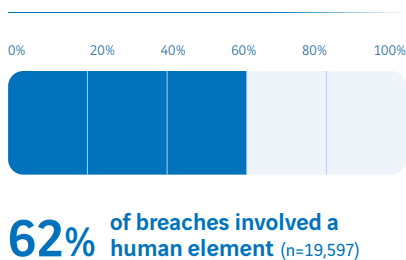


Figure 1: Select key enumerations in breaches
(2026 Data Breach Investigations Report,
Verizon 2026)

According to Axians SOC and incident-response teams, one of the strongest trends observed in 2026 was the continued **dominance of identity-based attacks**. Account compromise, credential theft and business fraud remained among the most common incidents investigated by our teams. In several environments, compromised business accounts were used to conduct credible fraud attempts through genuine communication channels and trusted relationships already in place. The lesson is clear: identity protection must now be treated as a first line of cyber defense. MFA, privileged access monitoring, identity governance and continuous detection should be prioritized before attackers turn trusted accounts into operational entry points.

Phishing campaigns also spiked. Indeed, attackers increasingly abuse legitimate business platforms and trusted services to host malicious content or redirect victims. *"In one recent pattern shared by our threat intelligence teams, attackers used services such as DocuSign to make the message feel routine, almost administrative. The end-user does not feel they are clicking on a suspicious link. They feel they are completing a normal business step"*, explains Stéphane Ben Oliel, Head of Cybersecurity Solutions at Axians France. The goal is to blend into normal business operations and exploit the trust users place in familiar tools. Awareness programs remain essential, but they must evolve continuously as attackers' techniques change.

Another major observation is the **acceleration of vulnerability exploitation**. Cloud adoption, remote access, connected services, and third-party integrations continue to expand digital footprints. Every new connection potentially expands the attack surface. The rise of AI is now acting as an accelerator. The gap between vulnerability disclosure and active exploitation continues to shrink, transforming patch management into a race against time. For more on AI in cybersecurity, see page 22.

In 2026, customers increasingly requested support with managing vulnerabilities, reducing exposure, improving patching processes and gaining greater visibility into their attack surface.

Data exfiltration also emerged as a major concern. While ransomware remains highly visible, many security teams are now equally focused on the theft of sensitive information. Large-scale uploads to cloud services, insider risks, and supply-chain exposure require continuous monitoring and proactive detection capabilities.

Demand also grew for **automation and AI-supported** analysis to manage the increasing volume and complexity of security events. Security teams are facing more alerts, faster attacks and shorter reaction windows than ever before. As a result, organizations increasingly rely on automation to accelerate detection, prioritize incidents, reduce response times and allow analysts to focus on investigation and decision-making rather than repetitive tasks.

"What often surprises customers is not how we get in, but how quickly a limited compromise can escalate once an attacker is inside. In our offensive security engagements, we regularly observe how a standard user account can become a pathway to much higher levels of access within hours, particularly when identity governance and Active Directory controls are not sufficiently mature. The real risk is often not the initial breach itself, but how far an attacker can move across the environment once trust has been compromised."

Alessandro Viscomi
Cybersecurity Offensive Specialist, Axians Italy



1.3 Preparing for the next wave

Looking ahead, **AI is the defining force shaping both attack and defense**. Attackers use AI-powered automation to accelerate information gathering, personalize phishing, improve social engineering, and create deep-fake content capable of bypassing traditional trust mechanisms. A realistic 2027 scenario does not necessarily involve a new type of attack, but the industrialization of familiar ones. An attacker controlling a compromised mailbox could analyze previous exchanges, reproduce the user's tone and language, impersonate a supplier, and initiate a fraudulent payment or data transfer. What once required time, language skills and manual preparation can now be accelerated with AI.

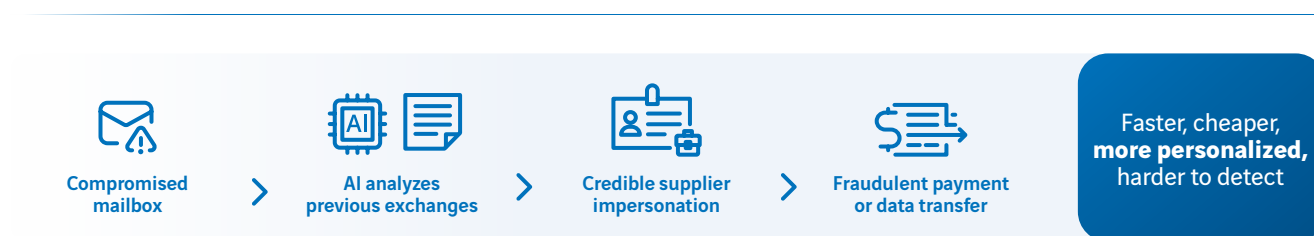


Figure 2: AI industrializes familiar attacks in the coming years (Source: UK National Cyber Security Center, the near-term impact of AI on the cyber threat)

Defenders must respond with the same level of innovation.

AI-assisted security operations, automated response workflows and intelligent alert prioritization will become essential capabilities rather than optional enhancements. Security teams cannot scale indefinitely through human resources alone; automation will be necessary to keep pace with the speed and volume of threats.

→ The threat landscape

Three priorities should guide cybersecurity investments in 2027.



Secure identities

Multi-factor authentication, identity governance, privileged access monitoring, Zero Trust principles, and continuous identity monitoring should form the foundation of any cybersecurity strategy.



Understand and control the attack surface

Organizations must know which assets are exposed across IT, IoT and operational technology (OT), maintain accurate inventories, and establish efficient vulnerability management processes. The principle remains true: organizations cannot protect what they do not know exists.



Invest in cyber resilience

Tested backups, recovery plans, crisis exercises, and supply-chain protection will determine how quickly organizations recover when incidents occur. Beyond resisting attacks, the objective is now to continue operating despite them.

The next attack may start with a stolen identity, an exposed asset or a trusted message.

The priority is to detect it early, contain it quickly and keep operating. Know your exposure. Monitor identities. Patch fast. Test recovery. **The objective is not to prevent every intrusion, but to stop one compromise from becoming a business-wide crisis.**

Governance, Risk and Compliance: From Obligation to Operational Resilience

2.1 Regulation extends beyond the IT department

Governance, risk and compliance (GRC) now extends beyond policies, audits and regulatory reporting. NIS2 widened the perimeter of cybersecurity, bringing many organizations, business services and operational environments into scope for the first time. In 2026, we continued to encounter organizations realizing that cybersecurity could no longer remain purely an IT topic. It now concerns production, quality control, supply chains, business continuity, executive decisions and the ability to keep delivering essential services.

At Axians, we believe that effective compliance starts with a risk-based understanding of the business, but NIS2 is not a checklist of technologies. It requires organizations to identify their critical activities, assess cyber risks, assign responsibilities, and decide which measures are appropriate to their context. This foundation then shapes security architecture, vulnerability management, incident response, supplier controls, and recovery capabilities.

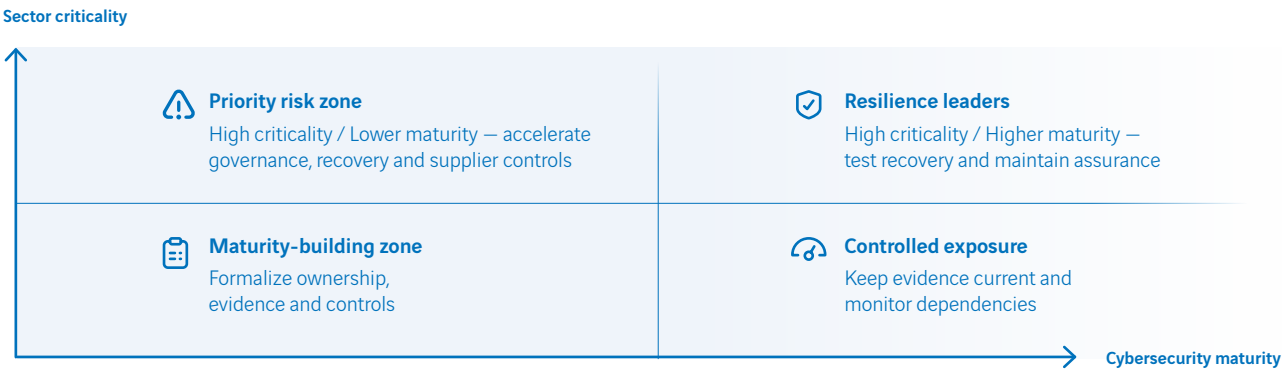


Figure 3: Cyber-Risk Map under NIS2 (source: ENISA NIS360 public approach - maturity vs criticality)

Cyber resilience completes this approach. Protection remains essential, but organizations must also prepare to withstand disruption, operate temporarily in a degraded mode, and recover their complete ecosystem. Many of them consider that there is only one server to restore. But cyber resilience goes further. It requires an acceptable level of business operation while people, processes, applications, infrastructure, and suppliers are being restored.



"Cyber resilience is tested by how smoothly the protect-detect-respond chain works and how effectively people act when systems, suppliers or critical services are disrupted. Plans that allow the business to keep operating at a minimum viable level through a disruption are just as important as recovering quickly and securely."

Dennis Martin

Business Resilience and Crisis Management at Axians UK

2.2 What 2026 revealed behind the compliance checklist

A first recurring gap was the **absence of a formal cyber risk-management** capability. Organizations struggle to define a methodology, identify risk owners or connect technical findings with business impacts. In some cases, even ownership of cyber risk, business continuity or OT security was unclear.

The second major challenge is **third-party risk**. Assessing suppliers is not limited to sending a questionnaire. It requires procurement, legal, security and business teams to work together on supplier classification, contractual security clauses, evidence collection, risk scoring and continuous monitoring.

"This long and complex process can be structured and industrialized by moving toward SaaS-supported tools that we use regularly", explains Francesco Serena, Cybersecurity consultant at Axians Italy. This illustrates how NIS2 is turning supplier governance from a one-off compliance task into an ongoing operating process.

A third gap also appears in **operational environments**. Some organizations still assume that segregated or supposedly isolated OT systems are outside the cybersecurity perimeter. Assessments frequently exposed legacy technologies, limited asset visibility, unclear recovery responsibilities and disaster-recovery plans that could not be tested without risking production. *"In one large manufacturing environment, traditional IT disaster-recovery methods could not be applied directly because of long-life production assets, restricted maintenance windows and plant-specific constraints"*, notes Francesco Serena. Recovery plans must reflect operational constraints rather than replicate traditional IT disaster-recovery models.

Our experience shows that resilience must therefore be designed across people, processes, and technology. This includes organizational and technical audits, exposure assessments, risk analysis, continuity and recovery plans, crisis-management procedures, vulnerability testing, security monitoring, and regularly exercised response scenarios.

Designing these capabilities is only the first step. Organizations also need to prove that they work when pressure is real. **Testing is therefore essential**. A backup, recovery procedure, or fallback mode is only credible when it has been verified. Tabletop exercises help organizations expose missing contacts, undocumented dependencies, unrealistic recovery objectives and processes that work on paper but fail under pressure. They also help define the minimum viable level of operation that must remain available during a disruption. *"Exercises help turn these plans into practical capability: teams understand their roles, escalation routes are clear, recovery decisions can be made faster, and gaps are identified and closed before a crisis hits"*, says Dennis Martin, Business Resilience and Crisis Management at Axians UK.

2.3 2027: Building governance for a broader risk landscape

In 2027, the scope of cyber governance will continue to expand. The Cyber Resilience Act will extend responsibility toward digital products and components throughout their lifecycle, including vulnerability monitoring and security maintenance after delivery. AI governance will add further requirements around data integrity, traceability, robustness, and protection against data manipulation.

Our recommendation is to avoid managing every regulation as a separate project.

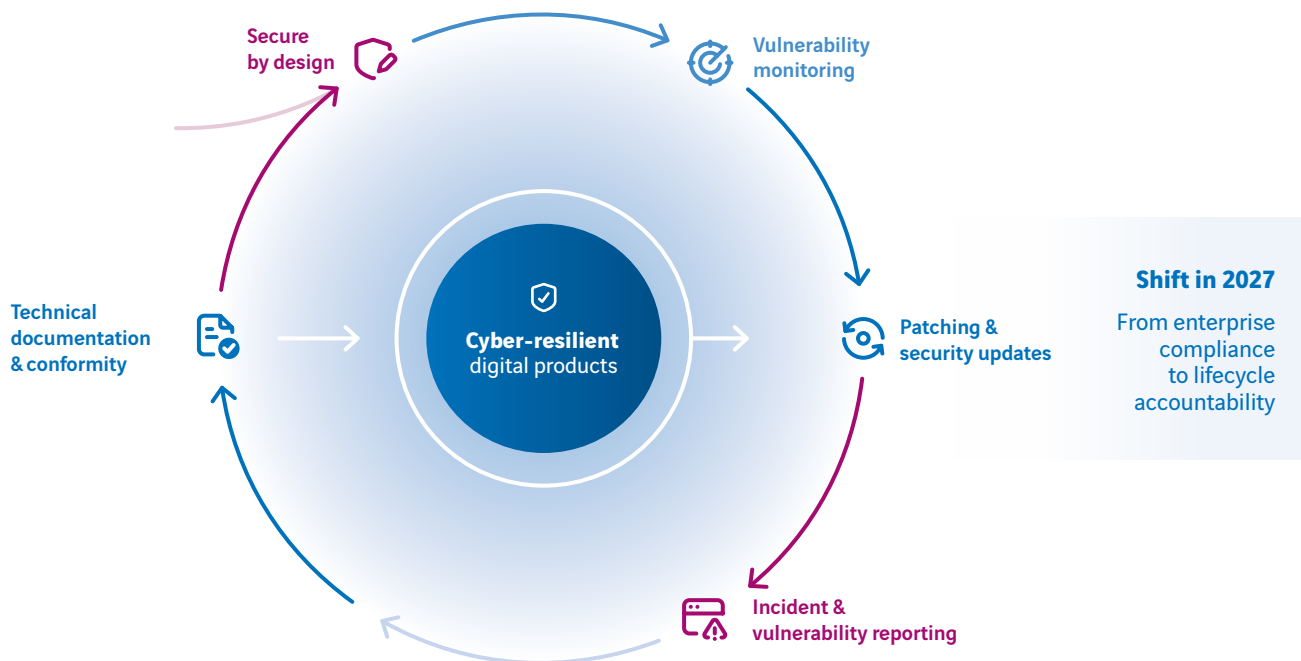


Figure 4: Cyber Resilience Act: product-security lifecycle (source: European Commission's public Cyber Resilience Act Guidance)



Governance, Risk and Compliance

A pragmatic roadmap should build a durable foundation around three priorities.



Establish executive accountability

Cybersecurity needs clear leadership, decision rights, and direct visibility at management level. It must connect IT, operations, legal, procurement, risk, and business continuity.



Operationalize risk and supplier governance

Maintain current asset and dependency information, prioritize risks, integrate security requirements into contracts, and continuously monitor critical third parties.



Prove resilience through exercise

Define minimum viable operations, build recoverable architectures and regularly test crisis, backup, restoration and communication procedures.

Governance creates value when it changes operational decisions. **As Axians combines consulting capabilities with hands-on technology expertise, we bridge the gap between governance frameworks and operational reality.**

The goal is not to produce more documentation but to help organizations make informed decisions, demonstrate control, recover confidence, and continue operating when conditions are far from normal.

OT Cybersecurity: From Operational Visibility to Board-Level Resilience

Across energy, manufacturing, transport, utilities, logistics and critical infrastructure, Axians teams have observed a fundamental shift in 2026: digitalization accelerated, IT and OT environments converged, and cybersecurity became increasingly tied to operational performance.

For decades, industrial organizations focused primarily on availability and safety. Cybersecurity has often been addressed through isolated projects such as firewalls, segmentation, remote access controls or physical separation between IT and OT. Today, the challenge is broader. Connectivity is increasing. Recovery plans must reflect operational constraints rather than replicate traditional IT disaster-recovery models. Production sites are exchanging more data than ever. Cloud platforms, remote maintenance, AI-enabled systems, and digitalized operations are becoming standard across an increasing number of industrial environments.

At the same time, many organizations are still asking a simple question: *"What exactly do we have in our OT environment?"*

3.1 Visibility remains the foundation of OT cybersecurity

Daily, we see the same pattern: Initial assessments often reveal that customers do not have a reliable view of their OT assets, legacy systems, or network flows. They should start with asset discovery, network-flow mapping, and dependency analysis to build a long-term roadmap. Nonetheless, organizations should not wait for perfect visibility before acting. Based on our experience, immediate improvements such as secure remote access, network segmentation, and resilience measures can reduce risk quickly while a broader cybersecurity program is developed in parallel.

In addition, we believe that OT cybersecurity is more than protecting industrial assets. It is also about protecting production continuity, operational resilience and business outcomes. And it starts with the stability and fault tolerance of the OT network itself. A single failed link, switch misconfiguration or uncontrolled Layer 2 interaction can have a direct impact on production. This is why OT cybersecurity can no longer be treated as a standalone technical topic. It is now directly connected to broader cyber priorities such as governance, threat management, AI-enabled risks, and evolving regulations.



"In industrial environments, cybersecurity progress is measured differently by operations, engineering, safety, IT, risk and compliance teams. The board's role is to ensure these efforts form a coherent risk and resilience position, with clear accountability, understood obligations, adequate funding and measurable improvement in safety, availability, compliance and continuity of service."

Marc Wren

Head of OT Cybersecurity at Axians UK

3.2 From technical controls to industrial resilience

Axians observes that OT cybersecurity is evolving from a technology-focused initiative into a broader business transformation program. Indeed, Axians' customers are moving beyond isolated technical deployments towards structured cybersecurity governance. **Regulatory requirements such as NIS2** have been a major catalyst: in many cases, what started as a compliance question quickly became a broader discussion about risk ownership, budgets, roles and business continuity.



Figure 5: NIS2 changes compared to NIS1 (Source ENISA NIS2 What you need to know)

Mature organizations increasingly combine technology, governance, and resilience initiatives. They still invest in network segmentation, industrial visibility tools, OT intrusion detection systems, secure remote access, and monitoring capabilities. In parallel, a growing number are engaging leadership teams, defining cybersecurity ownership and establishing multi-year improvement programs.

At an earlier stage of OT cybersecurity maturity, organizations often begin with the fundamentals: discovering assets, understanding network flows, identifying vulnerabilities and building their first OT cybersecurity strategy.

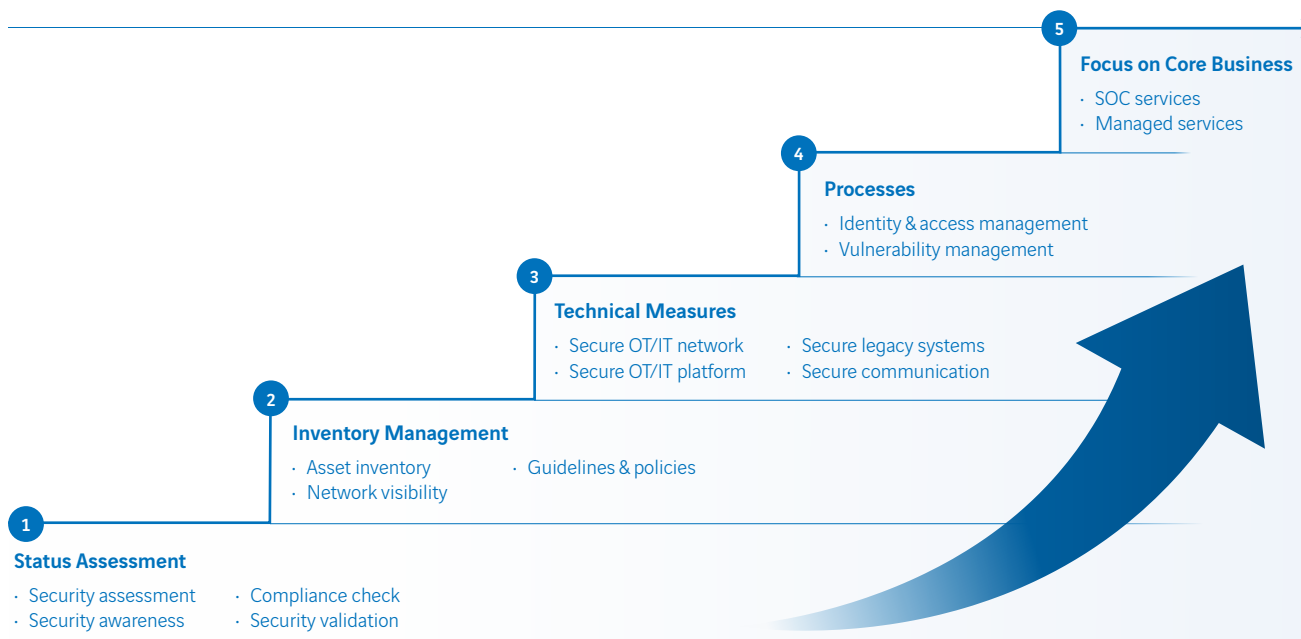


Figure 6: The main steps for a journey with Axians and VINCI Energies

A recurring theme across all geographies is the growing importance of **resilience**. Customers are no longer asking only how to prevent attacks. In some of our engagements, the key question from operations was more direct: *"Can we keep producing if something happens?"*

As a result, tabletop exercises, disaster recovery planning, cyber incident simulations, and business continuity programs have become increasingly common. Organizations want confidence that they can maintain operations or recover rapidly when disruption occurs.

Axians' experts have also observed significant growing demand for **secure remote-access solutions**. In many cases, customers discovered that multiple suppliers had access to industrial systems without a consistent governance model. As maintenance increasingly relies on external experts, controlling vendor access has become a priority. Similarly, network segmentation continues to deliver immediate value by reducing attack exposure and limiting operational impact.



Table 1: Best practices for remote access for Industrial Control Systems
(Source: ICS Recommended Practices CISA - Cybersecurity & Infrastructure Security Agency)

This also points to a growing need for consulting and advisory services. Our customers increasingly ask questions such as: *"Can you help us document what we need to do?"* or *"Can you show us the path forward?"* They expect **practical guidance, realistic roadmaps and measurable progress** rather than another technology deployment.

Delivering this kind of guidance requires a combined understanding of cybersecurity, IT and industrial processes. As part of VINCI Energies, Actemium, Omexom and Building Solutions activities, we understand not only cybersecurity technologies but also industrial processes, plant operations, energy infrastructure and operational realities. This allows us to translate cyber requirements into solutions that work in production environments.

"Our industrial clients struggle most with preparing their own organization for a cybersecure mindset. As long as it is "an IT problem", the required changes do not happen. As a result, large technological investments deliver limited value. Factory teams are often not ready to handle the increased complexity. Alternatively, clients can delegate cybersecurity improvement goals to their factories or quality departments. The operational teams become better prepared for the new cybersecurity tasks and will enable smarter technology investments."

Bert Schoofs

Business Unit Manager – Axians ICT for OT Belgium





OT Cybersecurity

Looking ahead, we believe that organizations must first establish solid foundations, combining technological architecture, including segmentation, DMZs, and secure remote access, with an organizational framework.

Building on these foundations, the next phase will be defined by three key priorities.



Governance

Will become a decisive success factor. OT cybersecurity initiatives increasingly require executive sponsorship, clear accountability, and dedicated budgets. Organizations that treat OT cybersecurity as a business risk rather than an IT project will move faster and achieve better outcomes.



Visibility

Will remain essential. As customers expand by acquiring new companies, while also digitalizing operations, integrating complex supply chains, and connecting more assets, their industrial attack surface continues to grow. Asset inventories, monitoring capabilities, digital twins, and real-time visibility solutions will play a growing role in maintaining control.



Resilience

Will become the primary objective. The focus is shifting from protecting individual devices to ensuring continuity across the entire OT ecosystem. In several projects, the real risk was not located inside a single PLC, but at the intersection of IT and OT: engineering workstations, remote access servers, shared access credentials, backup platforms, or unmanaged network connections.

We also expect regulations such as NIS2 and the Cyber Resilience Act to continue shaping priorities. Compliance alone will not be enough. Organizations will increasingly seek evidence of maturity, resilience, and measurable progress.



"As OT environments mature, the focus is expected to shift from assessment and remediation toward continuous monitoring, managed security services and OT SOC capabilities. A growing shortage of specialized OT cybersecurity skills will further accelerate this transition."

Alain De Pauw
Division Manager at Axians IT Security Germany

Finally, technology adoption will accelerate in several areas: OT monitoring, integrated IT/OT security operations, AI-assisted detection, secure remote access, segmentation, and virtual patching. This acceleration matters because **AI is shortening vulnerability** and exploitation timelines. The challenge is no longer only the zero-day vulnerability, but the risk of near-instant exploitation which could be described as the rise of the "zero-millisecond."

Customers do not need perfection from day one. They need a realistic roadmap, clear priorities and a trusted partner capable of combining strategic guidance with practical execution.

The future of OT cybersecurity belongs to organizations that combine industrial expertise, cybersecurity knowledge and operational resilience. Axians helps secure what matters most: operational continuity, people's safety and business resilience.

The New Cyber Perimeter: AI, Identity and Control

Artificial Intelligence has become part of everyday business operations. We have seen organizations deploying AI assistants, integrating large language models into business processes, automating workflows, and experimenting with increasingly autonomous AI agents. From a cybersecurity perspective, what distinguishes AI is not only the speed of its adoption, but also the entirely new attack surface.

Many organizations know that AI is in use, but few can accurately identify which models are deployed, what data they process, which agents are operating in the background or which business decisions depend on AI-generated outputs.

This lack of visibility creates a broader security challenge. Organizations are no longer protecting only users, devices, applications and data. They must now **secure AI models, AI-driven decisions, autonomous agents** and the information those systems can access.

AI security is rapidly becoming as much a governance and risk-management challenge as a technical one.

The organizations that will benefit most from AI will be those capable of balancing innovation with visibility, security, and accountability.

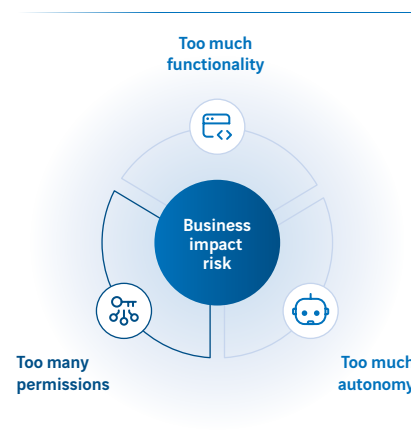


Figure 7: Govern AI agents like privileged identities

4.1 Visibility lost, governance required

In 2026, AI adoption continued to outpace governance, with employees, developers and business teams frequently adopting AI solutions without involving cybersecurity teams.

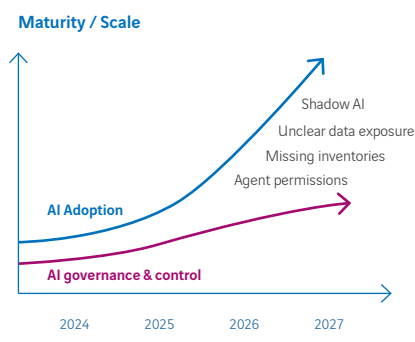


Figure 8: AI adoption is outpacing governance

We repeatedly observed employees, developers, and business teams adopting AI solutions independently of cybersecurity teams. *"The challenge is that end users treat AI like a search engine. They upload internal documents, request summaries, and only afterwards does the organization realize it has no visibility or control over what was shared"*, explains Ricardo Cavaleiro-Sousa, Line of Business Manager at Axians Digital Trust Portugal. This phenomenon, often referred to as **shadow AI**, creates significant challenges around visibility, data leakage, compliance, and risk management. The issue is rarely malicious intent; it is a lack of control over what data is shared, who shares it and which AI services are used.

As a result, one of the most common customer requests concerns visibility rather than advanced AI protection technologies. Organizations want to understand where AI is being used, which AI models are deployed, what data is being shared, and how to establish governance around these initiatives. We support customers through AI security assessments, AI inventories, governance frameworks, secure adoption roadmaps, and monitoring capabilities designed to identify uncontrolled AI usage and reduce data exposure risks.

Security attention is also shifting towards **AI-enabled applications** themselves. Traditional application security remains essential, but our experience shows that securing the application around an AI model is no longer sufficient. New attack techniques, such as prompt injection and abuse of large language models, are creating risks that many security teams are not prepared to address. This has increased demand for AI-focused DevSecOps practices, AI security assessments, model testing and controls designed specifically for LLM environments.

Another recurring discussion concerns **AI agents**. While they offer significant business value, they also create a new identity challenge. Indeed, *"an AI agent designed to automate a business process may need access to finance, sales and operations data. To make it work quickly, teams are often tempted to grant broader permissions than a human user would normally receive"*, observes Chris Gilmour, CTO at Axians UK. If compromised, such an agent could become a privileged entry point across several business silos. Identity governance, access management and privileged access controls have consequently become central components of AI security discussions with customers.

At the same time, AI is **strengthening cyber defense capabilities**. Our security teams, and those of our customers, increasingly use AI to analyze large volumes of events, improve detection quality, automate repetitive investigation tasks and accelerate incident response. AI is not replacing cybersecurity experts. It is helping them operate at a speed that better matches today's threat landscape. This is especially visible at Level 1, where analysts are shifting from repetitive alert handling toward higher-value investigation, validation and decision-support activities.

"AI is accelerating both sides of the cybersecurity arms race.

Attackers will always have greater freedom, but organizations can stay competitive by combining AI-powered defense with strong governance, identity-centric security, and resilience-by-design."

Chris Gilmour
CTO at Axians UK



4.2 Securing the age of autonomous AI

As AI adoption accelerates, we expect organizations to discover that **identity becomes the primary security control for autonomous systems**. Unlike traditional applications, AI agents require access to multiple data sources, business processes and external services to deliver value. In many environments, we already observe teams granting broad permissions to agents simply to make projects work faster. Over the coming years, this approach will become unsustainable. Organizations will need dedicated governance models for both human and non-human identities, combining Identity and Access Management (IAM), Privileged Access Management (PAM), authorization policies and continuous monitoring. At Axians we believe the defining security question of this era could be: "What is this agent allowed to do, access, and decide?"

We also expect organizations to move beyond isolated AI deployments toward ecosystems of **interconnected agents** capable of making decisions, interacting with systems and collaborating autonomously. This evolution will create new challenges around accountability, authorization, traceability, and trust. Organizations will increasingly need to explain how AI systems reach decisions, demonstrate control over AI actions, and govern interactions between agents operating across business boundaries.



Artificial Intelligence

Based on our global experience, organizations should now focus on three priorities.



Establish AI governance before AI adoption scales further

Organizations need clear ownership, security policies, inventories, risk assessments, and security-by-design principles before autonomous AI becomes embedded in critical processes.



Invest in identity-centric security

As AI agents proliferate, identity becomes the new security perimeter. Strong IAM (Identity and Access Management), PAM (Privileged Access Management), authorization models, and governance mechanisms for both human and non-human identities will be critical to maintaining control.



Build cyber resilience rather than relying solely on prevention

AI is accelerating attackers and defenders alike. Organizations should assume incidents will occur and focus on limiting impact through Zero Trust architectures, segmentation, AI-enhanced security operations, and rapid recovery capabilities.

One theme remains consistent:
AI is transforming cybersecurity faster than any previous technology wave.

The organizations that succeed will not necessarily be those deploying the most AI. They will be the ones capable of governing it, securing it, and maintaining trust in an increasingly autonomous digital world.

Quantum Security Starts With Knowing What to Protect

Quantum computing is the technology that could break today's cryptography; quantum security is the set of measures designed to keep data protected in a post-quantum world.

For years, quantum computing has been presented as a future disruption. In cybersecurity, however, the discussion is no longer theoretical. The question is not whether quantum technologies will eventually challenge today's encryption standards, but how organizations should prepare without overreacting.

At Axians, our experience shows that the first step is to separate reality from hype. For example, Quantum Key Distribution (**QKD**) and Post-Quantum Cryptography (**PQC**) are often grouped together under the label "quantum-safe security", yet they solve very different problems. Both technologies have a role to play, but not necessarily at the same time, and not for the same organizations.

Security leaders increasingly understand the risk of 'harvest now, decrypt later'. Encrypted information collected today could potentially be decrypted in the future once sufficiently powerful quantum computers become available. This concern is particularly relevant for organizations managing sensitive information with long confidentiality requirements spanning ten, fifteen, or even twenty years.

At the same time, quantum computing remains an emerging technology but most organizations are not preparing to deploy quantum networks in the near future. Instead, the most advanced companies are trying to understand where cryptography is used today, which systems could become vulnerable tomorrow, and how to build a realistic transition strategy. That is where cybersecurity, governance and long-term planning intersect.



FUNDAMENTAL PRINCIPLES

QKD (Quantum Key Distribution)

- Secures the exchange of encryption keys
- Capable of detecting interception attempts during the transmission process
- Requires dedicated infrastructure
- Mainly relevant for highly sensitive communications

PQC (Post-Quantum Cryptography)

- Replaces today's vulnerable cryptographic algorithms
- Works with existing infrastructures and products
- Becoming part of normal technology refresh cycles
- Relevant for almost every organization

5.1 Quantum in 2026: Simply curious, testing, or deploying?

We have seen a clear increase in customer interest in quantum-safe security. Organizations from public administration, financial services, critical infrastructure, academia and research ecosystems have started exploring the topic through workshops, assessments, laboratory environments and pilot projects.

Our experience shows that large-scale QKD deployments remain rare. Most projects are still proofs of concept, test beds or research initiatives designed to validate technology maturity and operational feasibility. *"This year, QKD was not only a topic we discussed with customers; it became something we worked on in real projects, through controlled point-to-point test environments designed to validate quantum-based key exchange."* explains Alejandro Diez, Head of Business at Axians Spain.

This confirms an important market signal: QKD is becoming tangible, but it is still mainly used to test feasibility, build expertise and understand operational constraints before any broader rollout. Universities, public institutions, innovation programs and highly regulated sectors continue to be the earliest adopters, often testing quantum-secure communications in controlled environments before considering operational deployment.

On the other hand, many organizations still lack a precise mapping of the cryptographic technologies they rely on today, from certificates, VPNs and PKI systems to encrypted communication channels and application dependencies. When customers ask how to become quantum-ready, the first challenge is rarely QKD, PQC or advanced mathematics. **The challenge is understanding where cryptography already exists.**

Across multiple engagements, we observed customers struggling to build inventories of certificates, VPNs, PKI, encrypted communication channels and application dependencies. Without this visibility, it is impossible to prioritize migration efforts, evaluate exposure, or determine which systems require protection first. Quantum readiness should start as a discovery exercise and not a technology deployment project.

Based on our engagements, a pragmatic roadmap is emerging:



This approach allows organizations to prepare without creating unnecessary disruption. We have also observed growing interest in vendor solutions that map certificates, manage cryptographic dependencies and support future migration initiatives. At the same time, customers increasingly want guidance, not just technology.

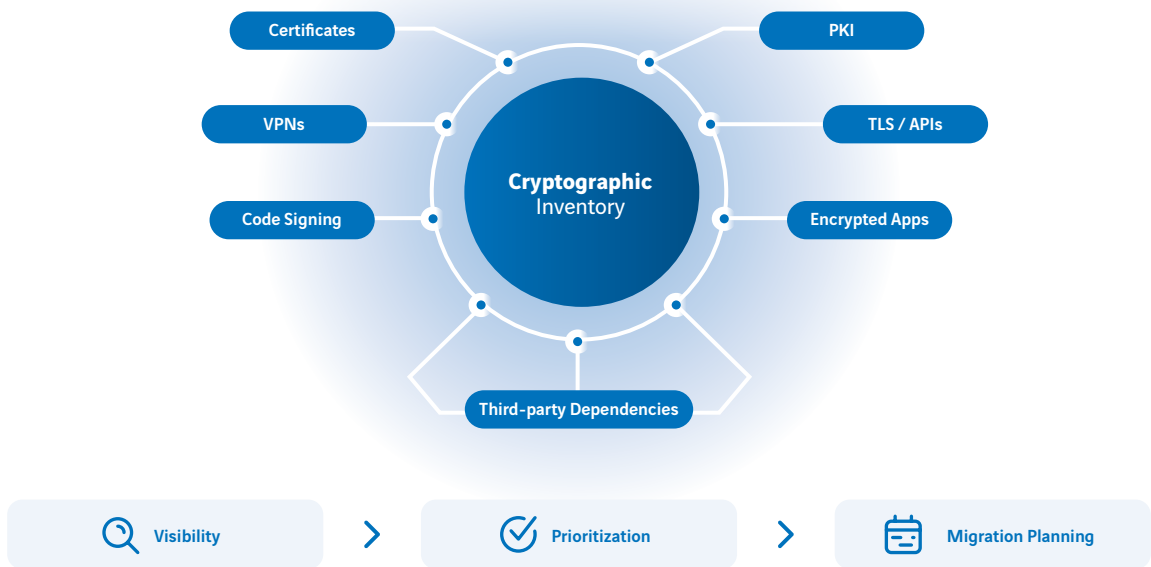


Figure 9: Cryptographic inventory is the starting point

This is where emerging risks need to be translated into practical, locally adapted actions. Our role is not to sell quantum technology for the sake of innovation. It is to help you understand your exposure, make informed decisions, and prepare your infrastructure for future requirements through realistic and achievable roadmaps.

5.2 Building quantum readiness before it's required

Over the next few years, PQC adoption is expected to outpace QKD adoption. Security vendors are already integrating post-quantum algorithms into firewalls, VPNs, and broader security platforms. As organizations refresh infrastructure and modernize security architectures, PQC capabilities will increasingly become part of standard product roadmaps.

QKD, by contrast, is likely to remain a strategic niche technology in the near term. Adoption will first accelerate in sectors where confidentiality is mission-critical, and information must remain protected for decades. Defense, government organizations, sovereign communications, and financial institutions are expected to remain among the leading adopters.

Organizations should avoid both panic-driven technology replacement and passive observation. The practical path is to build visibility, governance and a phased transition plan.

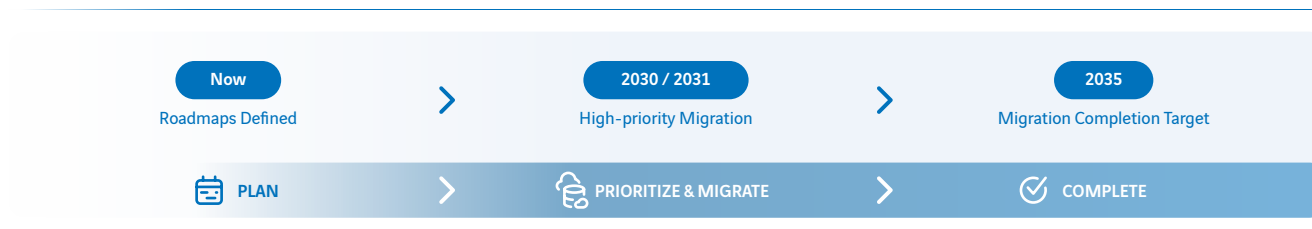


Figure 10: PQC roadmap timeline, Now › 2030/2031 › 2035



Quantum security:

Our recommendation for the next years is simple and starts now.

- **Build a complete cryptographic inventory.**
- **Create a quantum-readiness roadmap aligned with business risk.**
- **Ensure future technology investments are compatible with post-quantum cryptography requirements.**

The organizations that will be best positioned for the quantum era will not necessarily be those deploying the most advanced quantum technologies first. They will be the organizations that already understand their cryptographic landscape, can prioritize migration decisions, and have a clear roadmap for adapting as the market, vendors and regulations evolve.

Quantum security is not yet a race to deploy new technology everywhere. It is a race to understand where organizational risks are.

Building Resilience, Together

Throughout this report, one message is clear: cybersecurity challenges are now deeply interconnected. Identity, governance, infrastructure resilience, AI adoption and quantum readiness can no longer be addressed separately. Across industries, countries and customer environments, the priorities may differ, but the direction is the same: organizations must prepare better, adapt faster and recover with confidence.

At Axians, we combine international cybersecurity intelligence with local delivery and customer-facing expertise. Our strength lies in helping organizations translate emerging risks into practical actions adapted to their reality.

This report is not an endpoint. It is an invitation to continue the discussion, challenge perspectives and turn insight into action. Discuss your cybersecurity priorities with an Axians expert:

<https://www.axians.com/expertises/cyber-security/>

**Axians,
2026-2027**

€3.8B
in revenue

36
countries

16K
colleagues

385
business units



Figure 11: Axians key figures, 2026-2027.

Credits

This report was made possible by:

The international Axians Cybersecurity community, Cybersecurity experts, SOC managers and analysts, Threat Intelligence specialists, Security architects, Pentesters and Red Team experts, Governance, Risk & Compliance consultants, dedicated OT cybersecurity specialists, business leaders, Axians Cybersecurity Club members and VINCI Energies cybersecurity contributors.

Special thanks to all participating countries and experts who shared their experience, observations, and lessons learned to make this report possible.

Vincent BAZILLIO (Axians Cybersecurity Global Community Lead) – **Stéphane BEN OLIEL** (Head of Cybersecurity Solutions – Axians France) – **Fabio CAGNA VALLINO** (Business Unit General Manager – Axians Managed Services Italy) – **Cédric CAILLEAUX** (Business Unit Manager – Axians Cybersecurity France) – **Rui CALMAO** (Executive Director – Axians Portugal) – **Ricardo CAVALEIRO-SOUSA** (Line of Business Manager – Axians Digital Trust Portugal) – **Filip CIZMESIJA** (Business Unit General Manager – Axians Infrastructure & Cybersecurity Croatia) **Vincent CLOT** (Director – Axians France) – **Alain DE PAUW** (Director – Axians IT Security Germany) – **Alejandro DIEZ** (Head of Business – Axians Cybersecurity Spain) – **Niels EVERSTYJN** (Business Unit Manager – Axians Cybersecurity Netherlands) – **Moncef FARCHADO** (Business Unit Manager – Axians Morocco) – **Plinio FAVA** (Business Unit General Manager – Axians Brazil) – **Adolfo GARCIA YAGUE** (Business Development Manager – Axians Cybersecurity Spain) – **Chris GILMOUR** (CTO Axians UK) – **Wojciech GLINIECKI** (Infrastructure Director – Axians Poland) – **Benjamin GRAY** (Lead OT Security Engineer – Axians Cybersecurity UK) – **Florian GROESSL** (Deputy Division Manager – Axians Network & Cybersecurity Austria) – **Timmy HOPF** (Business Developer in OT Vertical – Axians IT Security Germany) – **Wilfried HOUTPUT** (Business Unit Manager – Axians Belgium) – **Loubna IZIKA** (SOC Manager – Axians France) – **Bertrand LECLERC** (Cybersecurity Director – VINCI Energies) – **Dennis MARTIN** (Head of Business Resilience – Axians Cybersecurity UK) – **Zoran OLUJIC** (Business Area Manager Cyber Security – Axians Germany) – **Javier PASTOR** (Business Development Manager – Axians Cybersecurity Spain) – **David PREINL** (Business Unit Manager – Cyber Analytics & Defense Axians Germany) – **Rudolph PREUSS** (IT-OT Coordinator – Actemium Germany) – **Jesus REQUENA** (Director – Axians Spain) – **David RODRIGUEZ** (Business Development Specialist – Axians Spain) – **Rosa Maria RODRIGUEZ** (Business Unit Manager – Axians Spain) – **Bert SCHOOF** (Business Unit Manager – Axians ICT for OT Belgium) – **Francesco SERENA** (Consultant – Axians Cybersecurity Italy) – **Florian STROEMMER** (Senior Network Engineer – Axians Network & Cybersecurity Services Austria) – **Benoit TIZIANEL** (CSIRT Analyst – VINCI Energies Systèmes d'Information) – **Michal VALACH** (Business Unit General Manager – Axians Cybersecurity Czech Republic) – **Joël VIALON** (Business Unit Manager – Axians Switzerland) – **Alessandro VISCOMI** (Cybersecurity Offensive Specialist – Axians Italy) – **Marc WREN** (Head of OT Cybersecurity – Axians Cybersecurity UK),

and the Axians Brand Team, especially **Laure BAUDOT** (Graphic Design Manager) – **Mourad KAMEL** (Content Manager) – **Carelle MOUKEMAHA** (Communications Manager).