
AXA
XL Insurance
Resilience at Scale
Cyber resilience in an era of consolidated & converging threats
Produced in partnership with THALES

Contents

Disclaimer

This report is the result of analysis from a wide variety of sources including publicly available reports, insights and analysis, and proprietary analysis and insights by AXA XL and Thales, based on their internal data. A non-exhaustive list of publicly available sources is included in the report but doesn't constitute the sole source of insights that made this report possible.

The analysis presented in this report is based on information available at the time of writing. When future evolution is expressed, it doesn't constitute prediction of the evolution of trends and threats, but the expression of the possible future context in which organisations may have to operate.

Foreword

Spending on cybersecurity has never been higher. Confidence in cyber resilience has never been lower.

In 2026, digital disruption is no longer a contained technical issue, but a defining feature of the current economic and geopolitical environment. Consolidated cybercrime, geopolitical tension, regulatory expansion, and rapid technological acceleration are all converging to reshape how organisations operate and compete.

Cybercriminal activity is more than ever a combination of coordination, sophistication, speed and scale. **Geopolitical tension increasingly plays out in the digital domain, where economic pressure, espionage and disruption intersect.** Regulatory frameworks continue to extend expectations of governance, resilience and transparency. And at the same time, advances in AI, automation and quantum computing are altering both defensive capabilities and adversarial tactics, as well as lowering barriers to entry for attackers.

The significance of cyber risk continues to grow. It influences supply chains, service delivery, investor confidence and cross-border trust. As our digital and physical worlds collide, the impact of a cyber breach now extends into physical consequences too. Interconnected ecosystems mean disruption rarely remains isolated anymore.

For boards and executive teams, the implications are clear: cyber resilience is now a core business priority. It influences risk, continuity and trust, and increasingly acts as a source of competitive advantage when volatile conditions arise. To be effective, it cannot sit solely within technical functions. It must be embedded across the organisation through clear accountability, strong governance, robust risk management and executive buy-in, with rehearsed response plans and greater visibility across the business.

This report examines the dynamics defining the 2026 cyber landscape and outlines priority areas for leadership to focus their attention on, to build sustained, business-wide resilience within their organisation.

Jonathan Salter,
Head of Risk Consulting

Rebiah Bardot-Girard,
Head of Cyber Risk Consulting Services

Executive summary

Business leaders are increasingly being held accountable for the cyber readiness of their organisations. The risk environment facing businesses in 2026 is changing, shaped by exponential acceleration in how threats emerge, scale and intersect with core business operations.

Four developments in particular are defining the cyber risk landscape in 2026, shaping what leadership must prioritise this year:

The consolidation of cybercrime's ecosystem

Cybercrime operates more than ever as a coordinated ecosystem. The efficiency and speed of cybercriminal groups is enhanced with the further professionalisation of this ecosystem and AI-augmentation of underlying tools. Average breakout times have fallen to under half an hour in many cases, meaning less time to react once a breach happens. Vulnerability and credential-based intrusions are still primary entry points, while the effects of a supply chain compromise can now scale far beyond a single organisation. Risk increasingly extends beyond corporate IT into operational technology (OT) environments, where attackers recognise the potential to cause operational disruption and physical consequences.

For leadership teams, actionable threat intelligence is central to an effective response in case of suspicious activities.

Geopolitical cyber escalation

The intertwining of digital activity and geopolitical competition has created another layer of complexity, with espionage, disruption and economic pressure acting alongside financial motivation to diversify danger. Organisations face an array of exposure threats beyond direct targeting today, with geography, sector alignment, and supplier relationships all potential routes to an attack.

Risk modelling must therefore consider unpredictable changes that go beyond typical company threats.

Regulatory fragmentation and sovereignty pressures

Long-proposed regulatory frameworks are finally coming into force and tightening expectations surrounding governance, resilience, reporting and executive oversight. From NIS2 and the AI Act in Europe, to parallel measures across other major markets, compliance obligations are reshaping operating models.

Technology sovereignty pressures are adding new layers of complexity too, with organisations facing increased scrutiny over the platforms, providers and infrastructure they rely on across different jurisdictions. This can limit which technologies are deployed in specific markets and complicate global operating models, requiring leaders to think more carefully about resilience and strategic dependencies.

Technological acceleration and systemic exposure

AI adoption is advancing rapidly across enterprise functions. While enabling efficiency and insight, it is also reshaping the threat landscape.

AI-assisted intrusion, impersonation and automation are increasing the credibility and scalability of attacks. Interconnected systems, adoption of IoT technology and machine-driven processes are also broadening potential entry points. Advances in quantum research are introducing longer-term considerations for cryptographic resilience as well, meaning organisations need to plan and prepare defences early.

What this means for business leaders:

Embed cyber defence into governance and strategy.

Board oversight should reflect the financial and operational materiality of digital risk, with cyber security integrated into enterprise risk management and long-term planning.

Strengthen oversight across dependencies.

Supply chains, cloud environments and OT can be hit hard and fast. Additional visibility is needed to ensure safety.

Prepare leadership to act under pressure.

Clear decision ownership, practised escalation routes, and a crisis response plan people trust, are essential when incidents move fast and impact needs containing.

Cyber resilience is about more than just surviving a cyber incident. It's about protecting enterprise value, sustaining stakeholder trust, and maintaining operational continuity. At AXA XL Cyber Risk Consulting, and in partnership with Thales, we support organisations in strengthening cyber readiness across the full lifecycle of cyber risk, translating complex threat insight into practical, integrated action.

The state of cyber risk in 2026

Cyber risk in 2026 is defined as much by operational disruption as by financial loss. The global average cost of a data breach still stands at a staggering $4.44m[1], combining initial investigation and remediation costs, as well as longer term impacts like sustained business interruption, regulatory response and reputational impact. For organisations operating across multiple jurisdictions, costs compound quickly when supply chains or shared platforms are affected.

The scale and frequency of attacks experienced today demonstrates that rather than coming in waves, threats are persistent. More than 12,000 confirmed data breaches were recorded globally in 2025[2] – the highest total on record. At the same time, vulnerability discovery continues at pace, with roughly 130[3] new common vulnerabilities and exposures (CVEs) published every day. Each new disclosure expands the attack surface organisations must now track, prioritise and remediate.

The speed of attacks is further shifting the balance too, with the average breakout time – the point at which an adversary begins moving laterally through a network – falling to approximately 29 minutes, with the fastest observed at 29 seconds[4]. While global median dwell time shows that attackers' actions may not be immediate, the speed at which a compromise can escalate once inside a business has materially increased.

The global average cost of a data breach:

$4.44M

[1] IBM, Cost of a Data Breach Report 2025
[2] Verizon, 2025 Data Breach Investigations Report
[3] DeepStrike, Vulnerabilities Statistics 2025
[4] CrowdStrike, 2026 Global Threat Report

Recent incidents illustrate just how quickly disruption can cascade through interconnected systems. In the UK, JLR was forced to shut down its IT Systems and halt global manufacturing operations for weeks. In the US, the Change Healthcare ransomware attack in 2024, triggered a weeks-long outage that disrupted claims processing across healthcare providers and pharmacies nationwide.

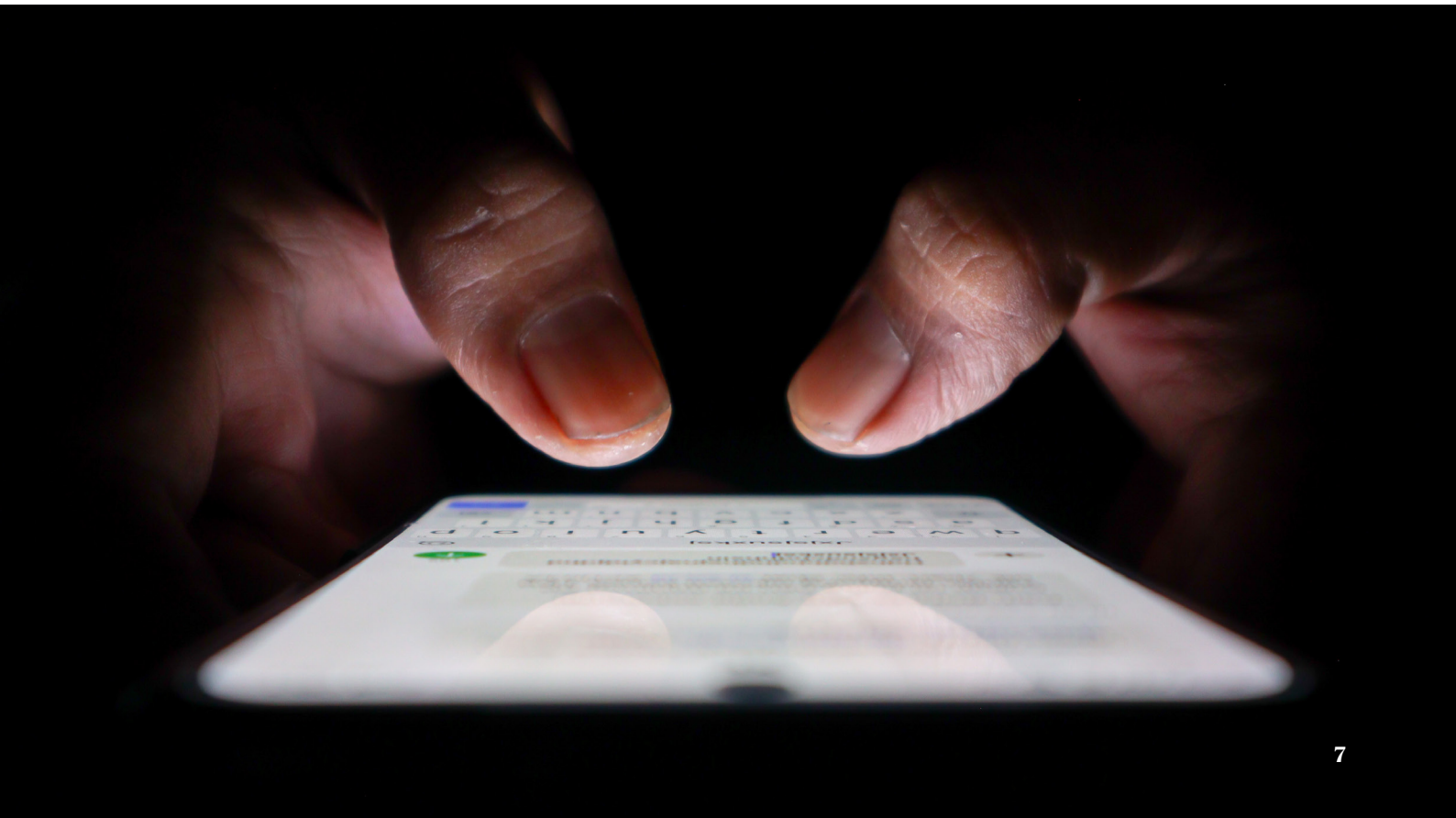
Attacks are now a constant feature of the threat landscape. For leadership teams, the challenge is not only preventing compromise, but ensuring disruption does not scale across the business and its wider ecosystem.

Average breakout time now:

29 minutes

Artificial Intelligence has fundamentally changed the economics of cybercrime, turning it into a highly industrialised sector. We are no longer just facing human adversaries, but AI-powered 'malware-as-a-service' and automated ransomware campaigns capable of adapting in real-time. This technology has drastically lowered the barrier to entry for attackers while multiplying their speed of execution. When you combine this automated scale with state-sponsored actors and geopolitical tensions, the threat landscape becomes unprecedented. Today, companies must defend against an ecosystem that is faster, cheaper, and more relentless than ever before.

Ivan Fontarensky,
CTO, Thales



Consolidated cybercrime

Cybercrime now operates as a structured, adaptive and commercially organised ecosystem.

Ransomware-as-a-service is no longer an emerging trend but an established operating model, enabling developers to distance themselves from frontline operations while affiliates carry out intrusions and extortion. The same logic now extends across a broader criminal marketplace, including phishing-as-a-service, access brokerage and other specialist capabilities sold on demand. In some cases, this division of labour has evolved further still, with negotiation support offered as a service to help manage ransom demands and payments. The result? An accessible, specialised and scalable attack economy.

Recent threat reporting suggests access broker advertising grew by 50% through 2024, reinforcing how quickly initial access has become commoditised[5]. Coordinated law enforcement has achieved notable success in disrupting major ransomware groups, reinforcing the value of collaboration. However, even when a collective is disrupted, it often only fragments, reforming under new branding, preserving tools and expertise, while rebuilding infrastructure.

AI is now intensifying models too. Generative AI tools, including malicious variants such as WormGPT, are being used to craft phishing campaigns, generate exploit code and automate reconnaissance. These allow attackers to finetune messages to sound convincingly human, iterate quickly when something fails, and push high-volume campaigns at speed with little overhead.

Hyper personalisation is simplified too with LLMs able to replicate styles and invoke references that appeal to different target groups with ease.

When it comes to social engineering, deepfake voice cloning and synthetic video are now deployed in social engineering campaigns, enabling attackers to impersonate senior executives or trusted partners with credibility. The surge in high-profile campaigns seen in 2025, such as those linked to groups like Scattered Spider, show how effective impersonation and help-desk manipulation have become, and why these tactics will persist in 2026 and beyond.

Supply chains present strategic leverage points too. Rather than targeting organisations directly, adversaries are compromising shared technology providers, managed service partners, or widely deployed platforms. Increasingly, they are also showing greater interest in OT environments, recognising the leverage that disruption to manufacturing, logistics and critical processes can create. Furthermore, vendor privilege, cloud misconfiguration, overextended access rights and global supplier reach can significantly expand the blast radius of a breach. Finally, regulatory scrutiny further raises expectations that organisations must understand and manage the safety of their third-party ecosystem.

The result is not simply a greater number of attacks, but a more efficient attack economy. Barriers to entry are lower, execution is faster, and impact now scales like never before. For businesses, this raises the odds of being caught up in something from a distance, shortens the time available to detect and contain, and increases the potential for operational and financial fallout.

[5] CrowdStrike, 2026 Global Threat Report

What this means for leadership

Consolidated cybercrime has changed the economics of risk and created a wide set of challenges for leaders. Speed, automation, and third-party dependency now shape exposure, and the knock-on effects expand across finance, technology, and governance, each bringing its own level of complexity.

For the CFO

Financial impact extends beyond ransom payments. Prolonged disruption, regulatory scrutiny and recovery investment can materially affect earnings and capital planning. Risk modelling must reflect more than just isolated breach events, taking into account systemic interruption as well.

For the CISO

Priority shifts beyond perimeter defence, to visibility of access pathways, credential control, third-party privilege, and rapid detection to reduce lateral movement and contain the attack radius.

For the Board

Oversight must move beyond compliance reporting to resilience testing. Directors should understand critical dependencies, escalation pathways, and whether leadership is prepared to act decisively under pressure.

For the Brokers

Exposure is harder to ringfence, and the loss profile is less predictable. Third-party and systemic disruption, rapid escalation, and higher recovery costs make it tougher to price risk, set terms, and validate controls with confidence.

Geopolitical cyber escalation

Cyber activity is increasingly embedded within geopolitical competition, making it a complex and growing threat vector. The distinction between criminal enterprise, hacktivism and state-aligned operations has become harder to define. Groups that appear to be independent activists may in fact be operating with quiet state tolerance or a degree of strategic alignment, while financially motivated actors sometimes overlap with national interests or broader strategic objectives.

The surge in hacktivist campaigns – often linked to regional conflict or ideological positioning – has expanded the attack surface for multinational organisations today. It means that targets are selected for their symbolic or strategic impact just as much as their commercial value. That makes incidents harder to manage, because organisations can face actors operating with a level of capability, protection or impunity that sits outside traditional risk assumptions.

Exposure is also less tied to a company's own actions; businesses may find themselves targeted because of geopolitical events, government decisions or legislative changes in their country. It signals a more politicised threat landscape where brand, operations and reputation can be pulled into events well beyond the company's control.

This pressure is especially visible in critical infrastructure. Energy grids, water utilities, maritime logistics and transportation networks are regularly probed for vulnerabilities, with OT now a growing focus because of its potential to create real-world disruption. Many of these environments rely on OT designed around availability and safety first. These systems are often expected to run for years or decades, and changes may require downtime, validation and recertification, making them harder to update at the pace of corporate IT and potentially leaving vulnerabilities exposed for longer. As digital and physical systems converge, a compromise can move quickly from data loss to tangible disruption, including prolonged service disruption, public safety risk and economic instability.

Cyber operations are also being used as instruments of economic pressure. Digital sabotage, industrial espionage and intellectual property theft can erode competitive advantage without overt escalation. The intent isn't always to steal data. In some cases, the point is the disruption itself, or the reputational hit that follows, which can amplify uncertainty among investors, partners and customers.

For business leaders, neutrality no longer guarantees insulation. Geographic footprint, supplier relationships, perceived country of origin and sector alignment may influence exposure irrespective of intent. Organisations must plan for being pulled into events they didn't choose, with supply chains becoming a common pressure point and regulators increasingly expecting clearer visibility across the full dependency chain, extending beyond third parties to fourth, fifth and even further-tier relationships.

The implication is strategic. Business leaders need to incorporate geopolitical escalation into risk modelling, crisis planning and insurance strategy, so that plans reflect the realities of political and economic volatility today. Without this, they risk being caught unprepared when tensions spill into the digital domain, leading to slower response, greater operational disruption, and sharper financial and reputational damage.

> Operational technology or Internet of Things environments present a very different cybersecurity challenge from traditional IT systems, as many were not originally designed with cybersecurity in mind. As these systems become more connected to cloud services and digital platforms, the potential attack surface is expanding significantly. A cyber incident affecting an operational environment can quickly translate into disruption of manufacturing lines, energy systems or transportation networks, which is why resilience is so vital. In critical infrastructure in particular, the objective is not just to stop attacks, but to maintain safe and continuous operations thus staying aligned with regulations.
>
> **Ivan Fontarensky,**
> **CTO, Thales**

Critical infrastructure in the cyber crosshairs

Energy

Energy infrastructure remains a high-value target due to its economic and societal impact.

Maritime

Attacks on port and logistics networks can affect cargo flows, shipping schedules and global supply chains.

Healthcare

Healthcare systems remain a major ransomware target. The 2024 Change Healthcare attack disrupted payments and claims processing across the US healthcare sector.

Regulatory fragmentation and sovereignty

Cyber risk now is being shaped by regulatory expansion as much as by threat activity. Privacy and data protection laws are in effect in 144 countries[6], with new cyber and AI frameworks continuing to emerge across major markets. Within the European Union alone, NIS2, the AI Act, DORA, and the Cyber Resilience Act, significantly extend organisational obligations, tightening reporting timelines and raising expectations around governance maturity.

Regulation now sits at the centre of strategy, with surveys indicating that 96% of executives report strengthening security posture in response to regulatory pressure[7], reflecting the growing alignment between compliance and operational preparedness. Enforcement is also becoming more assertive, increasing the financial and reputational consequences of governance failure.

Technology nationalism is another pressure set to define 2026 and beyond. As governments seek greater control over strategic technologies, organisations

144 countries

now enforce privacy or cyber regulation

may face growing constraints over which providers, platforms and infrastructure can be used in specific markets. This goes beyond data location alone; it affects cloud strategy, vendor selection, resilience planning and the ability to maintain standardised global operating models.

At the same time, data sovereignty considerations are introducing new operational complexity. Around 70% of EU cloud deployments are controlled by US-headquartered providers[8], creating tension between localisation expectations and cross-border service models. That pressure increases further when European regulatory regimes intersect with US legislation such as the CLOUD Act, intensifying scrutiny over data access and jurisdictional control.

[6] IAAP, Global Privacy Law and DPA Directory
[7] PWC, 2025 Global Digital Trust Insights
[8] Synergy, European Cloud Provider research

Quantum computing represents a long-term structural shift in cybersecurity, not a distant theoretical problem. The risk organisations face today is what we call the 'harvest now, decrypt later' scenario, where attackers collect encrypted data now with the intention of decrypting it once quantum capabilities mature. This approach means organisations must start preparing today, by building robust inventories to understand what data is being encrypted, particularly for systems and products that will remain in use for the next decade or more.

Ivan Fontarensky,
CTO, Thales

Compliance today sits within a growing, interdependent regulatory web. For businesses, it means assessing what data they process while facing added scrutiny over where it resides, how it moves, and which legal regimes assert authority over it. The cost of compliance is material, but the cost of non-compliance – including fines, litigation and loss of market access – is potentially greater.

Regulatory change is also unfolding in distinct waves. The end of the 2010s was defined by privacy and personal data, leading to the rapid expansion of data protection laws worldwide. The first half of the 2020s has centred more on resilience, with frameworks such as NIS2 and DORA likely to shape regulatory thinking well beyond Europe. The second half of the decade is set to focus increasingly on AI, as the EU opens the way and other jurisdictions introduce their own approaches. For organisations, keeping pace with these successive waves, while anticipating the next one, is becoming a strategic requirement.

For leadership teams, regulation shapes how organisations are governed, how technology is designed, and how resilience is built. This requires leaders to treat regulatory change as a strategic planning input, aligning legal, risk, and technology teams early, building compliance into system design, and making sure governance structures can respond quickly as new rules emerge.

Technology evolutions and systemic risk

Technological acceleration is reshaping both opportunity and exposure for organisations, and the pace of change is starting to outstrip current controls.

AI is being deployed at scale across a plethora of industries, improving productivity, automation, and insight generation. At the same time, organisations are managing a growing estate of connected devices across IT, IoT and operational environments, increasing the number of entry points that need to be secured. Against that backdrop, 2025 marked a visible shift in AI's weaponisation. Generative models are being used to automate reconnaissance, refine phishing campaigns, and develop exploit code, while early forms of autonomous intrusion agents demonstrate how attack tooling may evolve.

Brand impersonation risk is climbing in parallel, as the tools that make content cheaper and faster also make it easier to fake communications, websites and trusted brand interactions. Motives extend beyond financial gain, with bad actors also setting out to cause customer harm and reputational damage. As a result, organisations need to scrutinise activity conducted in their name, communicate clearly with customers and strengthen trusted communication channels.

Executive and employee impersonation are also becoming more credible. Deepfake voice cloning, synthetic video and other AI-enabled tactics are increasingly being used to imitate senior leaders or staff to bypass trust-based controls and gain privileged access. As digital identities become easier to manipulate, verification mechanisms and user awareness need to evolve.

Looking further ahead, a different kind of risk is starting to take shape. Quantum computing introduces

a structural challenge for businesses in the future, threatening to weaken encryption mechanisms protecting data. The immediate threat isn't that today's systems can suddenly be broken; it's that, over time, powerful quantum machines may be able to crack widely used public-key encryption, exposing sensitive data and undermining trust mechanisms such as digital certificates and secure connections. But while post-quantum solutions are emerging, the transition itself is likely to be complex, costly and prolonged, requiring organisations to update cryptographic dependencies embedded across systems, products, vendors and infrastructure.

In practice, the more immediate timeline may be shaped less by the technology itself than by regulation and compliance expectations. As governments and regulators in markets such as the US, EU and UK begin setting clearer expectations around post-quantum readiness, organisations may find that the pressure to transition comes before the threat is fully tangible. Organisations should be mapping where encryption is used across systems, vendors, and products today, so that a move to post-quantum cryptography can be planned in good time.

In the meantime, other foundational risks persist, with 60% of breaches involving a human element[9] and the vast majority of cloud security failures linked to customer misconfiguration. The gap between awareness and secure behaviour remains material for companies, despite years of advice and education about threats.

The internet is becoming ever more machine-dominated too. Agentic AI, automated APIs and proliferating IoT devices are all creating autonomous data flows at scale. Agentic AI in particular, is likely to mark the next major shift in reshaping how organisations deploy AI internally, and how malicious actors automate targeting, decision-making and intrusion.

Innovation continues to drive value, but without structured governance, it can also amplify systemic vulnerability. That impact shows up in faster incidents and more disruptive knock-on effects across systems. The priority is to set clear ownership and bake security into identity, cloud configuration and third-party controls before change outpaces oversight.

[9] Verizon 2025 Data Breach Investigations Report

The leadership imperative

In an environment defined by accelerated attack cycles, regulatory scrutiny and deepening interdependence, cyber resilience can no longer sit solely within technical functions. It is a governance responsibility that demands clear ownership, established escalation pathways, and leadership that has rehearsed its response before an incident occurs.

Durability now reflects how well risk is embedded into organisational decision-making, capital allocation, and oversight structures. The issue is no longer whether incidents occur, but whether leadership is structurally prepared to contain them.

These priorities are not abstract governance ideals. They determine whether disruption is absorbed, contained and learned from, or whether they influence an organisation's operations, performance and potential future.

Key questions for the Board:

- *Are we prepared for geopolitical retaliation that could affect operations or supply chains?*
- *Do we have a clear inventory of our cryptographic assets and dependencies?*
- *Are our security controls and resilience practices adequate to sustain and quickly respond to digital disruption?*

Five strategic priorities for 2026:

Ensuring full visibility of digital assets and exposure. Boards require a reliable view of the organisation's digital footprint, including OT, cloud environments, and third-party dependencies. Without clarity on what is connected, which systems are critical, and where sensitive data resides, risk can't be meaningfully prioritised or mitigated.

Having stronger third-party and ecosystem oversight. Interconnected supply chains mean exposure often sits outside the traditional perimeter. Governance frameworks must extend to vendors, managed service providers, and shared platforms, with resilience expectations embedded into procurement, contracting, and continuous monitoring.

Certainty that AI governance matches adoption speed. AI is being deployed across functions faster than oversight structures evolve. Leadership should define acceptable use, establish accountability for model outputs, and ensure data integrity, identity assurance, and auditability are embedded into AI-enabled processes.

Being crisis ready at board level. Response capability can't be theoretical. Executive teams need clarity on decision rights, regulatory obligations and communication protocols under pressure. Scenario exercises and escalation rehearsals are essential disciplines to have.

Being deliberate about a post-quantum transition roadmap. While large-scale quantum disruption is not immediate, cryptographic exposure must be mapped early. Long-life data, encryption dependencies and migration pathways necessitate structured oversight to avoid reactive and costly transition later.

These priorities are not abstract governance ideals. They determine whether disruption is absorbed, contained and learned from, or whether they influence an organisation's operations, performance and potential future.

The AXA XL approach

Cyber risk now moves faster than most organisations can react, requiring a comprehensive, lifecycle-based approach to resilience – one that anticipates and responds to emerging vulnerabilities.

AXA XL's approach is designed to guide clients through this dynamic environment by integrating risk assessment, preparedness, protection and response into a cohesive framework. This structured methodology ensures that organisations can identify vulnerabilities early, enhance their defences, and recover swiftly from incidents, ultimately supporting sustained business resilience amid uncertainties. Our goal is to translate insights into actionable strategies that strengthen long-term cyber resilience.

AXA XL's four-pillar framework offers a holistic approach to cyber resilience, designed to help organisations proactively manage risk, respond effectively to incidents, and sustain business continuity. Each pillar focuses on critical stages of the cyber risk lifecycle, delivering outcomes that strengthen governance, safeguard reputation, and ensure operational resilience.

Prevent

Prevent is the foundational pillar, emphasising the importance of proactive risk management. It involves comprehensive risk assessments, compliance evaluations and maturity diagnostics to identify vulnerabilities before they can be exploited. Strategic advisory services align cybersecurity initiatives with business objectives, helping organisations develop robust policies and control frameworks. The primary outcome is an enhanced security posture that reduces the likelihood of breaches, improves regulatory compliance and builds stakeholder confidence, creating a resilient environment that minimises operational and reputational risks.

Prepare

Prepare centres on readiness and resilience-building. This stage includes vulnerability identification, where organisations uncover weaknesses in their defences, and crisis simulations that mimic real-world attack scenarios. Regular readiness exercises & training foster a culture of preparedness, ensuring teams understand their roles and can respond swiftly and effectively during an incident. The benefits are improved response capabilities, minimised operational disruption, and maintained stakeholder trust, even in the face of adversity. This pillar ensures organisations are not just reactive, but ready to act decisively when threats materialise.

Protect

Protect involves continuous monitoring and active defence measures. By leveraging threat intelligence, organisations gain real-time insights into emerging risks and attacker tactics. Defensive controls, IAM (Identity and Access Management), EDR (Endpoint Detection and Response) help prevent unauthorised access and contain threats at their source. The outcome is a dynamic, layered security environment capable of detecting, blocking and mitigating attacks early, thereby reducing potential damage, safeguarding critical assets, and protecting brand reputation. This ongoing vigilance preserves business continuity and regulatory standing.

Prevail

And finally, Prevail focuses on incident response, recovery, and ongoing resilience diagnostics. When a cyber incident occurs, rapid and coordinated action is vital to limit damage and restore normal operations. Incident response planning, combined with resilience diagnostics, helps identify gaps and areas for improvement, ensuring organisations can bounce back quickly and learn from each event. Data privacy measures further protect sensitive information, maintaining customer trust and regulatory compliance. The goal is to turn every incident into an opportunity for improvement, safeguarding long-term reputation and operational stability.

The benefits of an integrated advantage

AXA XL's integrated advantage lies in its comprehensive, end-to-end approach to cyber resilience, setting it apart in the industry. By seamlessly integrating risk assessment, prevention, response, and recovery within the policy lifecycle, AXA XL ensures clients benefit from continuous, proactive support that evolves alongside their needs. This holistic coverage reduces gaps, enhances governance, and delivers measurable business outcomes, such as improved continuity and reputational protection. Within AXA XL, risk consulting acts as a critical interface between clients and underwriting too, translating on-the-ground risk assessments and mitigation advice into technical insights that support underwriting decisions on policy terms, pricing, and risk selection.

A key differentiator is the embedding of proactive services – such as threat intelligence, vulnerability management, and crisis simulations – into every stage of the cyber risk journey. These services empower organisations to anticipate threats, strengthen defences, and respond swiftly when incidents occur. AXA XL's global capability means clients gain access to local expertise backed by a worldwide network, ensuring tailored support regardless of geographic location or industry sector.

AXA XL's focus on OT alignment addresses the unique risks faced by industrial environments, integrating standards like IEC 62443 to bolster resilience in critical systems. Collaboration with technology leaders, notably Thales, enhances this ecosystem by integrating advanced security solutions and intelligence tools, providing clients with innovative, technology-driven insights.

Together, these elements create a unified, agile platform that not only mitigates risk but also accelerates recovery and long-term resilience. This integrated approach ensures organisations are better prepared for evolving threats, able to adapt swiftly, and capable of maintaining stakeholder confidence – an essential competitive edge in today's complex digital landscape.

The Thales approach

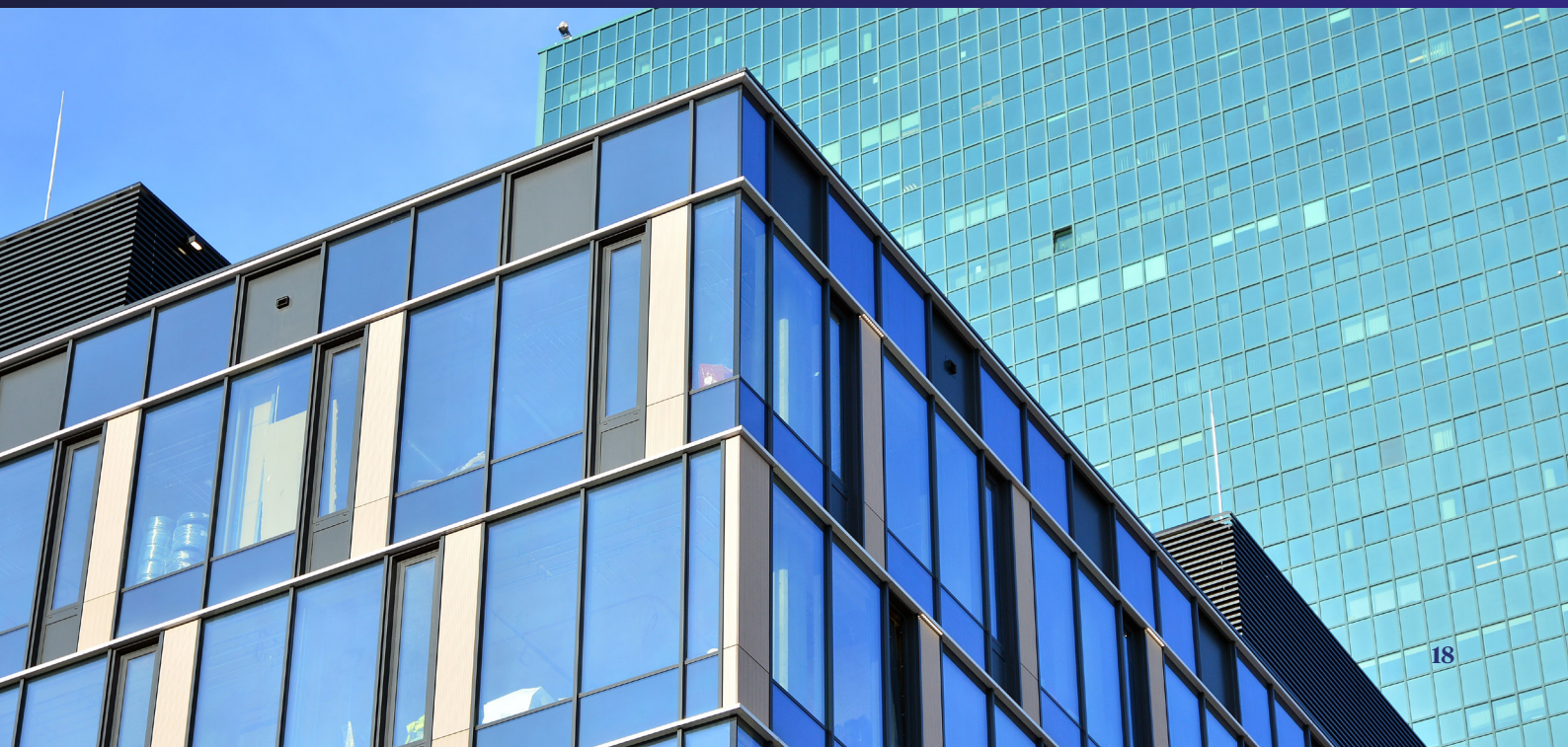
Ivan Fontarensky,
CTO, Thales

Attackers today are not simply becoming greater in number, but faster, more organised and more efficient, due to AI accelerating the speed at which vulnerabilities are now discovered and exploited.

In today's threat landscape, businesses need clear visibility of their most critical assets and vulnerabilities. Thales combines strong data protection, identity security and trusted infrastructure, with the flexibility to adapt as threats evolve – from AI-driven attacks to the future impact of quantum computing. By embedding security and sovereignty from the outset, enterprises can protect sensitive information, maintain operational continuity and build lasting digital trust. The most underestimated risk today is not a single technology, but the scale and speed at which attacks are evolving.

Delivering resilience through partnership

Cyber resilience can no longer be achieved through technology alone. It requires accurately quantifying risk and insuring against business impact. Our partnership with AXA XL bridges this gap, combining deep technical telemetry with financial risk modelling to support the entire cyber lifecycle.



Here are five areas enterprises must examine in 2026

1 Getting post-quantum ready

Quantum computing has the potential to disrupt the very cryptographic foundations that secure today's digital systems, yet many organisations lack visibility on where cryptography is used across their infrastructure, applications and products. Enterprises need to treat the quantum threat like any other security risk, with boards prioritising building robust inventories to understand what assets they own, and what data is being encrypted. Identifying long-lived IT systems and products that will remain in production for years is key to this process, as these are particularly exposed to 'harvest now, decrypt later' risks. Quantum is not tomorrow's problem – it a design challenge for today. If organisations start building cryptographic agility now, they can evolve securely as new standards emerge.

2 Expanding insight into digital sovereignty and trusted infrastructure

Geopolitical fragmentation is forcing organisations to rethink how they manage digital infrastructure, with data increasingly becoming a matter of sovereignty as governments place greater emphasis on where sensitive information is stored, and exactly who controls access to it. Today, true digital sovereignty extends far beyond the physical location of servers. It is about maintaining exclusive cryptographic control over critical assets – data, encryption keys, and identities – even within public or hybrid cloud environments. Organisations must assess which information is highly sensitive and apply 'sovereignty-by-design' principles, allowing them to take advantage of the scalability of the cloud without ever compromising control.

3 Examining risks surrounding identity erosion and impersonation

AI is transforming identity threats at pace, with deepfakes and AI-driven impersonation making it increasingly difficult for companies to verify digital interactions. We are now entering a world where the first question for any digital interaction will become: is this really a human I am interacting with? Soon traditional authentication alone will not be enough. Organisations need to start looking at new mechanisms to verify and protect identity, requiring layered approaches that combine strong authentication, behavioural monitoring and processes to protect sensitive communications.

4 Securing critical infrastructure and OT environments

The convergence of IT and OT has created efficiencies throughout many companies, but this shift has brought with it a wave of new vulnerabilities. As these environments become increasingly connected through cloud services and AI-driven systems, the potential impact of cyber incidents is growing at pace. Manufacturing is emerging as one of the most frequently targeted sectors, reflecting the growing value of operational disruption which can quickly translate into real-world consequences. Resilience in operational environments requires a new approach, supported by deep understanding of sector-specific threats. Businesses would be wise to start examining these now.

5 Shifting mindsets surrounding compliance

When every organisation now faces the prospect of attack, the real differentiator has become the ability to respond quickly and maintain operational continuity. Cybersecurity must move beyond merely focusing on compliance. Investment needs to be made not only in protection, but resilience too – ensuring systems, services and digital platforms remain available during disruption. This also requires securing AI systems and digital tools too, given increasing reliance on them. Those that embed security into their digital fabric today will not only reduce risk, but also strengthen confidence amongst customers, partners and regulators.

Final reflections

Cyber risk in 2026 reflects deep structural shifts in what companies have faced in previous years. Interdependence across technologies, supply chains and geopolitics now means disruptions spread quickly, with consequences that reach far beyond the initial breach area. Operational interruption, regulatory exposure and reputational damage are now more closely linked than ever, increasing pressure on leadership teams across the globe to respond with clarity and discipline.

For those reasons, cyber resilience now sits firmly within executive responsibility. It belongs in enterprise governance and operating design, supported by clear ownership, better visibility across critical assets and dependencies, and leadership teams that know how to act under pressure.

In this environment, resilience is also closely tied to trust. Customers, partners and regulators increasingly judge organisations by their preparedness, and by how well they maintain continuity when such events occur.

The priority now must be practical action. Improving visibility across digital estates and strengthening oversight of third parties will make organisations more resilient over time, as will more deliberate governance around AI and early preparation for the post-quantum transition.

With the right combination of advisory support, insurance insight and technology expertise, organisations can respond more effectively to current threats today and build a stronger long-term approach to the cyber risks of tomorrow.

Global Discliamer

Global Asset Protection Services, LLC, XL Catlin Services SE and their affiliates (“AXA XL Risk Consulting”) provide loss prevention and risk assessment reports and other risk consulting services, as requested. In this respect, our property loss prevention publications, services, and surveys do not address life safety or third party liability issues. This document shall not be construed as indicating the existence or availability under any policy of coverage for any particular type of loss or damage. The provision of any service does not imply that every possible hazard has been identified at a facility or that no other hazards exist. AXA XL Risk Consulting does not assume, and shall have no liability for the control,
correction, continuation or modification of any existing conditions or operations. We specifically disclaim any warranty or representation that compliance with any advice or recommendation in any document or other communication will make a facility or operation safe or healthful, or put it in compliance with any standard, code, law, rule or regulation. Save where expressly agreed in writing, AXA XL Risk Consulting and its related and affiliated companies disclaim all liability for loss or damage suffered by any party arising out of or in connection with our services, including indirect or consequential loss or damage, howsoever arising. Any party who chooses to rely in any way on the contents of this document does so at their own risk.

The information contained herein is intended for informational purposes only. Insurance coverage in any particular case will depend upon the type of policy in effect, the terms, conditions and exclusions in any such policy, and the facts of each unique situation. No representation is made that any specific insurance coverage would apply in the circumstances outlined herein. Please refer to the individual policy forms for specific coverage details. This summary does not constitute an offer, solicitation or advertisement in any jurisdiction, nor is it intended as a description of any products or services of AXA XL.

AXA XL is a division of AXA Group providing products and services through three business groups: AXA XL Insurance, AXA XL Reinsurance and AXA XL Risk Consulting. In the US, the AXA XL insurance companies are: AXA XL Insurance Company Americas, Greenwich Insurance Company, Indian Harbor Insurance Company, XL Insurance America, Inc., XL Specialty Insurance Company and AXA XL Excess & Surplus Lines Insurance Company. In Canada, insurance coverages are underwritten by XL Specialty Insurance Company - Canadian Branch. In Bermuda, the insurance company is XL Bermuda Ltd. Coverages may also be underwritten by Lloyd’s Syndicate #2003. Coverages underwritten by Lloyd’s Syndicate #2003 are placed on behalf of the member of Syndicate #2003 by Catlin Canada Inc. Lloyd’s ratings are independent of AXA Group. Not all of the insurers do business in all jurisdictions nor is coverage available in all jurisdictions.

axaxl.com