



Cyber security in 2027

resilience through strategic governance
and autonomy

forv/s
mazars

Foreword

Cyber security faces a convergence of rapidly shifting technologies, evolving regulations and advanced threats. To prepare for what's next, organisations will need to embrace strategic governance and intentional innovation.

This year's report explores how organisations can leverage technology and navigate complex global issues – like regulation, geopolitical instability and questions of digital sovereignty – to improve organisational resilience and autonomy.

To move forward, organisations must embed cyber security into their innovation and implementation strategies while staying agile to adapt to evolving threats. Those that do will protect their assets and gain a competitive edge in the digital economy.

As organisations look ahead to 2027, cyber security is increasingly inseparable from digital transformation. AI is reshaping the threat landscape, while operational shifts, regulation and digital sovereignty add further complexity. Together, these pressures are creating new risks and requirements that demand more strategic decision-making.

“Cyber threats are evolving faster than ever, driven by AI, interconnected ecosystems, geopolitical tensions and an increasingly complex regulatory environment. Yet the answer remains constant: a risk-based approach that protects what matters most and treats resilience, not simply compliance, as the true measure of cyber security.”



Wadi Mseddi,
Group Head of Cyber Security
Consulting, Forvis Mazars

Key insights

Leading organisations are moving beyond cyber security as a cost centre and finding strategic ways to leverage it as a competitive advantage

Digital sovereignty is an ever-increasing focus, but autonomy is a more useful objective for global organisations

A plethora of digital and security regulations in Europe and contrasts with a pull towards deregulation in the US, meaning a risk-based approach remains the answer to compliance fatigue

Operational technology is being integrated more and more into corporate IT ecosystems, creating both risk and reward

AI has created an arms race between attackers and defenders, necessitating fighting AI with AI and deploying right-sized governance

Data governance is still the cornerstone of effective cyber security strategies but must be applied proportionally

Cyber security teams must receive continual investment to balance stability with staying agile and advancing security postures



Global state of cyber security

Why cyber security is becoming a supply chain priority

Organisations with strong cyber security postures are increasingly winning contracts and partnerships over competitors, as RFPs and tenders now routinely screen out vendors who cannot demonstrate they meet prescribed cyber standards.

With the tech infrastructure and supply chain of each organisation growing more complex, organisations with strong cyber postures are increasingly benefiting from reputational advantages and supply chain preferences. This trend is particularly pronounced in B2B markets, where RFPs and tenders now routinely include substantial cyber security requirements, removing potential vendors from consideration whose cyber measures do not meet the prescribed standard.

The complexity of modern supply chains means that organisations often do not fully understand where their data resides or how it is being processed. This lack of visibility creates significant vulnerabilities, particularly as technologies like AI introduce new forms of data sharing and processing. Additionally, the growing interconnection between core enterprise systems, cloud platforms and third-party services is expanding attack surfaces and making resilience dependent on visibility across the full technology ecosystem.

Ultimately, each organisation is now expected to manage and monitor cyber security risks across its full ecosystem. This is reflected in the EU's Digital Operational Resilience Act (DORA) and the NIS2 Directive, both of which strengthen the requirements for managing third-party and supply chain cyber risks.

This shift towards shared responsibility is driving the adoption of more sophisticated third-party risk management (TPRM) frameworks. The rise of third-party monitoring tools that score organisations on cyber security metrics has created a new form of market pressure. Companies are discovering that their cyber maturity can directly impact their ability to win contracts, secure partnerships and maintain customer trust.



Global state of cyber security

Sovereignty versus autonomy: the new geopolitics of cyber security

Cyber security is increasingly a matter of national sovereignty. Governments now scrutinise where critical data is stored, who operates key digital services and which technologies organisations depend on, because cyber-attacks have become instruments of statecraft. Groups such as Volt Typhoon have embedded themselves in civilian infrastructure for future leverage, and disruptions like the 2024 CrowdStrike outage have exposed the fragility of over-dependence on external providers, especially those beholden to other jurisdictions.

The policy response has been swift, particularly in Europe: data residency requirements, sovereign cloud initiatives and a tightening web of regulation, with NIS2 and DORA emphasising operational resilience and supply chain security. The trend reaches well beyond Europe, however, and the bar for effective cyber security is shifting with it. From proving compliance to proving resilience, demonstrating that essential operations can continue and recover following a cyber incident is vital.

Yet sovereignty alone is not a resilience strategy. Pursued to its extreme, sovereignty can fragment supplier landscapes, duplicate infrastructure and limit access to effective technology, and can even concentrate risk, allowing a single government the power to hold continuity hostage.

What organisations should pursue is autonomy – the ability to understand, control and, where necessary, change their digital dependencies.

Framed this way, autonomy – not sovereignty – is the strategic objective, and a truer marker of the resilience regulators, customers and investors are really asking for.

Organisations should:

1

Know where sensitive data is stored and processed: including backups and support functions, not just what the contract says.

2

Understand suppliers' geopolitical exposure: hidden dependencies deep in the supply chain can matter as much as headline contracts.

3

Consider provider location and jurisdiction during procurement: the legal and geopolitical exposure of a critical provider is now a legitimate risk factor.

4

Demonstrate resilience, not just compliance: folding sovereignty into a broader resilience programme as one input among many.

“Organisations that treat digital sovereignty as one consideration within a deliberate pursuit of autonomy – knowing their dependencies, choosing trusted partners and proving they can withstand disruption – will find themselves not just compliant, but genuinely resilient.”



Jakob Haesler
Global Head of Consulting,
Forvis Mazars

“The boundaries between peace and conflict are blurring in cyberspace. State actors are positioning themselves inside civilian infrastructure – not for immediate gain, but for future leverage – and that changes the risk calculus for every organisation that depends on digital services.”



George Lagarias
Chief Economist,
Forvis Mazars



Global state of cyber security

How are DORA and NIS2 changing cyber security regulation?

DORA and NIS2 are reshaping cyber security compliance across Europe, shifting the standard from providing compliance on paper to demonstrating operational resilience. For multinational organisations, navigating both simultaneously has become one of the most complex regulatory challenges of 2027.

In the EU, the challenge is largely one of volume: [there are now well over a hundred digital-related acts and directives on the books](#), each adding to a dense, interconnected web of obligations. NIS2 is finally being enforced after several postponements, and the forthcoming Cyber Resilience Act will require products with digital elements to meet cyber security controls. Since NIS2 is a directive, member states write its principles into national law in subtly different ways, so organisations cannot simply lift and reuse compliance work from one jurisdiction to the next. The proposed digital omnibus aims to layer regulation more sensibly and tailor it to each organisation's size and risk profile, though it has yet to fully land.

Across the Atlantic, the problem inverts. The United States is moving towards significant deregulation, with nothing resembling a comprehensive federal framework for cyber security. What exists is principally industry- and government-focused, most notably the Cybersecurity Maturity Model Certification (CMMC) for those working with the Department

of War. Though, even this has been pushed back, its application effectively paused and the effects rippling into adjacent areas such as IT in financial services. There is no federal privacy law; protection is handled state-by-state, and the current political climate points away from national legislation rather than towards it. Counterintuitively, this lighter-touch environment brings its own fatigue: where some frameworks are highly prescriptive and others leave organisations guessing. Meanwhile, global businesses face the strain of reconciling wildly disparate approaches at once.

How a risk-based approach supports continuity without undue cost

This regulatory complexity has created what many industry professionals describe as both a burden and an opportunity. While many new regulations do aim to help improve resilience and business continuity, the burden compliance creates can also be a huge weight for already constrained teams.

As the web of compliance requirements becomes more complex, organisations who take a tick-box approach may struggle to juggle disparate requirements and convoluted areas of overlap. To remain cost effective in their compliance efforts, businesses should prioritise risk-based assessments. A risk-based cyber security approach can help cyber security teams focus on the risks that matter most, so compliance supports security instead of driving it.

“Compliance measures are just one variable in a risk-based cyber security program. A piece of regulation or a specific framework may impact the risk profile of one aspect of the business, but it shouldn't define the entire strategy.”



Tom Tollerton
Principal, CMMC Practice Lead,
Forvis Mazars in the U.S.

Global state of cyber security

What is operational technology security, and why is it under attack?

Operational technology (OT) underpins critical infrastructure and industrial operations worldwide. As these systems become more digitally connected, cyber threats are growing, exposing environments that have historically received less security attention than conventional IT systems.

OT has long been treated as an engineering concern rather than a cyber security one, protected less by sophisticated defences than by sheer isolation. However, attacks on OT environments are rising sharply, especially in critical infrastructure, and these historically under-protected systems are proving an attractive target for well-resourced, geopolitically motivated adversaries; December 2025 alone saw attempted attacks on infrastructure in both Venezuela and Poland. Set alongside incidents such as those at M&S and Jaguar Land Rover, where business continuity was significantly disrupted by cyber attacks, the expectation of visibility is only increasing.

Here lies a difficult paradox: most technology leaders report a serious lack of visibility into their OT network, and an organisation cannot govern what it cannot see. The natural response is to reach in and connect systems, data and other tools so that risk becomes legible and reportable. Yet, that reaching-in is precisely what creates the new exposure. OT environments are increasingly linked to corporate IT, cloud platforms and remote maintenance tools, and every new pathway erodes the isolation that may have been protecting these assets. The pursuit of transparency, handled without discipline, can manufacture the very vulnerability it was meant to expose – a risk compounded by OT's long lifecycles, legacy-by-default estate and huge change windows.

However, protecting these assets is becoming increasingly mandated by digital regulation, especially where critical infrastructure is concerned.

“The drive for OT visibility is necessary, but it has to be disciplined. When long-isolated systems are brought further online without proportionate governance and controls, organisations can increase the operational risk they are trying to understand and avoid.”



Paul Truitt
Principal, Cyber Security Practice
Leader, Forvis Mazars in the U.S.

Global state of cyber security

How is AI changing cyber security?

AI is changing the nature of cyber security on both sides of the battle. Attackers are using it to launch more sophisticated and targeted threats at scale, while defenders are leveraging it to strengthen detection, automate responses and improve resilience.

So far, AI has often been framed as opportunity versus risk, but that framing no longer holds. AI is a structural disruption transforming the entire landscape, and on both sides of the cyber fence, AI-driven ecosystems are emerging: from autonomous vulnerability discovery to fully automated attack chains. The result is an arms race in which the gap between attackers and defenders is widening.

An asymmetric contest

It's a possibility gap as much as a capability one; attackers and defenders may command similar technology, but agile attackers, by nature, often have the edge over process-bound defenders. Attackers have nothing to maintain: no business continuity burden, no change management, no regulatory obligations and no board to answer to. Defenders are bound by layers of policy, process and ethics – rightly so, because they have an organisation to protect – but every layer adds friction, and friction is precisely

what AI-enabled attackers exploit. The evidence of acceleration is everywhere:

- **Rising volume and realism:** The overall volume of attacks is climbing, with AI-leveraged fraud a particular growth area. Deepfakes have moved from novelty to boardroom threat – in one high-profile case, engineering firm Arup lost around \$25 million after an employee was deceived by a deepfake video call impersonating senior executives.
- **Self-rewriting malware:** Metamorphic malware – malicious code that rewrites itself to evade detection – is rendering traditional signature-based controls obsolete, forcing defenders towards behavioural indicators of compromise rather than known fingerprints.
- **Fully automated attack chains:** With agentic AI now capable of automating entire attack sequences, no human team can match the pace, no matter how strong its defences. Organisations need to patch proactively, monitor continuously and focus first on the systems and data that would cause the most damage if compromised.

If attackers are using AI, defenders must, too – and the good news is that it works.

“With agentic AI now capable of automating entire attack sequences, the result is clear: no human team can match the pace, no matter how strong their defences. So, while defenders are unable to take the same fully unbridled approach to AI usage, leveraging technology to scale their human capabilities is essential moving forward.”



Ali-Sultan Kirgizbaev
Partner, Head of Data & AI Centre
of Excellence, Forvis Mazars

Global state of cyber security

According to the [IBM “Cost of a Data Breach” report 2026](#), organisations using AI-assisted detection and response have seen the average cost of a breach fall by nearly 40%, with roughly \$1.93 million saved per incident, and the same techniques attackers use can be turned inward to stress-test an organisation’s own defences.

The ambition, increasingly, is agentic: AI that not only detects a threat but isolates and addresses it, with a human in the loop for critical decisions. Agentic AI can help address a key paradox of this arms race: deploying AI safely requires clear guardrails, but cyber security exists precisely because attackers exploit the unknown; defenders cannot pre-establish guardrails for every response a defensive agent might face. Attackers, on the other hand, face no such constraint. Agentic AI, appropriately harnessed, can respond to attacks semi-autonomously without the need for a crystal ball.

That said, the efficiency gains are real, but so is the risk; an attacker’s agent needs no permission structure, while a defender’s must work within justifiable guardrails.

“Taking the human out of the loop entirely is a massive concern. An agent must perform thorough validation on any input and establish guardrails against misuse throughout the system.”



Sean Andrews
Manager, IT Risk & Compliance,
Forvis Mazars in the U.S.

AI also expands the battlefield: every AI tool creates another attack surface, with prompt injection now mainstream – as DPD discovered when customers manipulated its chatbot into swearing at them, and McDonald’s when a recruitment chatbot exposed millions of applicants’ data. This is why AI governance and data privacy, long treated as separate if tangential disciplines, now urgently need consolidating into a unified policy, controls library and vendor oversight strategy.



Global state of cyber security

AI challenges & practical implementation strategies

The key challenges with agentic AI lie in confirming proper input validation and preserving meaningful human oversight, without letting it become a brake on every action.

As with all cyber security, AI governance should remain risk-based and proportional; it has never been possible to defend completely, and automated attacks only make that clearer. Security by design, the gold standard of risk mitigation, involves trade-offs with usability and time to market, and demanding perfection is self-defeating.

“Demand perfection, and you don’t get perfect security. You get a security function that becomes a blocker to doing business, workarounds that create shadow risk and defenders so burdened by compliance that they cannot do their actual jobs.”



Anton Yunussov
Head of Cyber Security Practice,
Forvis Mazars in the UK

The goal is not to eliminate risk but to identify the “crown jewels” and protect them proportionately. Cyber teams should act as business partners, enabling the organisation to adopt AI safely and at pace. In practice, that means:

Govern proportionately: apply the same risk assessment methodology used for other technologies, matching controls to the risk each AI use case carries. Not every deployment warrants the same scrutiny, and treating them as though it does makes failure more likely.

Keep humans in the loop: define what an agent may do on its own – identify, isolate, even shut down certain systems – and where a decision must escalate to a person, with robust input validation.

Consolidate governance and privacy: manage AI governance and data privacy together – shared policy, controls library and vendor oversight strategies – rather than as separate disciplines with separate metrics.

Invest in the team: upskilling cyber teams to keep pace with new attack techniques and defensive tooling is crucial; the capability gap is as much about people as technology.

Global state of cyber security

Quantum computing: preparing for the paradigm shift

While quantum computing may not pose an immediate threat to most organisations, the potential impact is so significant that preparation should begin imminently.

Understanding the quantum threat

The quantum threat operates on a different timeline than traditional cyber security risks. While quantum computers capable of breaking current encryption standards may be years away from widespread availability, adversaries are already employing “steal now, decrypt later” tactics.

“Cyber criminals are preparing for quantum computing now, so organisations should be too. They don’t need a quantum computer to act. They just need your encrypted data, and they can steal that today and decrypt it when the hardware catches up. The question isn’t when quantum will break your encryption, it’s how long your data needs to remain confidential.”



Anton Yunussov
Head of Cyber Security Practice,
Forvis Mazars in the UK

This reality means organisations should begin preparing for the transition to quantum-safe encryption, starting with cryptographic inventories, risk prioritisation and vendor roadmaps, before the threat becomes acute. The National Institute of Standards and Technology (NIST), having finalised its post-quantum standards in August 2024, has started to release quantum-safe cryptography tools and provide organisations with useful guidance for this transition.

Organisations can and should pursue quantum preparation now with cryptographic discovery and migration planning, beginning with the following steps:



Cryptographic inventory: map all systems and data that rely on cryptographic protection to understand potential vulnerabilities.



Asset prioritisation: identify which data and systems would be most severely impacted by a loss of cryptographic protection.



Transition planning: develop migration strategies for moving to quantum-safe algorithms as they become available.



Supply chain assessment: ensure that vendors and partners are also preparing for the quantum transition.

Global state of cyber security

Data strategy, transformation and governance

The “garbage in, garbage out” principle needs addressing more urgently than ever, as AI-driven decisions rely on high-quality data which consequently makes governance central to cyber security. Poor data governance creates cascading risks that extend far beyond

traditional data protection concerns. During incidents, organisations often discover previously unknown data stored in unmonitored locations with unclear access controls.

This lack of visibility not only creates unknown attack surfaces – data that is not properly catalogued cannot be adequately protected – but it can also create compliance risk.

Third-party risk management and data sharing

As data sharing grows more complex, TPRM has become essential to managing cyber risk. Multi-layered supply chains often obscure how data is processed and protected, increasing exposure. Effective TPRM requires several key components:

- ✓ **Service level agreements (SLAs) with security controls:** contracts should explicitly define security and compliance requirements, with the right to audit included wherever possible rather than relying on self-reporting.
- ✓ **Regular assessment and monitoring:** TPRM programmes can be more effective when they include ongoing monitoring and regular reassessment of vendor risks, and the right to audit only has value when it is leveraged.
- ✓ **Tiered vendor management:** not all vendors pose the same risk. Organisations should implement tiered approaches that focus intensive oversight on the most critical relationships.

Practical data security and governance implementation

Organisations looking to improve their data governance should consider starting with practical exercises rather than abstract policy development. Business continuity exercises can start around a table with leaders, technical and non-technical alike, opening with a simple question like, “what happens if your phone and computer do not work?” This more casual discussion can evolve naturally into more sophisticated dialogues about data dependencies and protection requirements.

This conversational approach extends to official policies as well. Cyber teams should consider whether policies are simple enough for non-technical users to understand and implement. Education and partnership can help both enable the workforce to uphold these policies and empower governance teams with the business knowledge they need to design effective measures.

“Security teams should work closely with business units to understand their data needs, develop suitable solutions and explain policies. When people understand the ‘why’, and when they trust that cyber teams understand what they are trying to achieve as well, they’re more likely to comply with security measures.”



Christopher Hock
Director,
Forvis Mazars in Germany

Global state of cyber security

This balance between data security and business enablement is a core governance challenge. Overly strict policies often lead to risky workarounds, fuelling the rise of shadow IT. An effective approach to workforce enablement combines technical controls with cultural initiatives. Close partnership with business units can create mutual understanding, and compensating controls like monitoring can keep cyber teams informed of user behaviour.

Cyber teams and expertise

The cyber security workforce faces unprecedented challenges as the field evolves rapidly and the skills gap continues to widen. Organisations need professionals who understand both traditional security principles and emerging technologies, but such expertise is increasingly rare.

The Chief Information Security Officer (CISO) role in particular has evolved significantly over recent years. CISOs are increasingly expected to function as business leaders rather than technical specialists, with responsibilities extending to regulatory compliance, board reporting and strategic planning. This evolution reflects cyber security's transition from a technical function to a business enabler.

The compensation for CISO roles has increased accordingly, reflecting both the expanded responsibilities and the importance of the role. However, this trend also highlights the challenge of developing a pipeline of qualified candidates who possess both the technical expertise and business acumen required for modern cyber security leadership. Many organisations are turning to virtual CISOs as a solution to help close gaps within their existing talent pool and provide a broader context of experience.

The innovation challenge

One of the most significant workforce challenges lies in finding professionals who can both innovate and manage, especially in medium-sized organisations. The rapid pace of technological change means that cyber security professionals should continuously learn new technologies while maintaining expertise in fundamental security principles.

This challenge is particularly acute in areas like AI and quantum computing, where the intersection of cutting-edge technology and security creates complexities that few professionals fully understand. Organisations are increasingly turning to trusted advisors and consultants to bridge this expertise gap, helping guide both strategy and implementation alongside internal teams.

Building sustainable cyber teams

The traditional approach of hiring individual cyber security experts is becoming increasingly unsustainable for many organisations. The competition for top talent is driving compensation to levels that many cannot sustain, while the rapid pace of change makes it difficult for internal teams to stay current with emerging threats and technologies.

Automation and AI are, of course, enabling cyber teams to scale their operations, but shared service models are increasingly common, particularly in scenarios involving mergers and acquisitions, where parent companies or investment firms provide cyber capabilities and support for portfolio/child companies. External partnerships are also increasingly valuable, bringing proven implementation approaches and helping organisations fill expertise gaps cost-effectively.

“CISOs must now be able to quantify the business value of cyber security, communicate effectively with non-technical executives and align security strategy with business objectives. This takes a lot of hard and soft skills – not to mention experience – that many organisations can't afford until long after they need it.”



Jan Matto

Senior Advisor Digital Trust, Former
Partner, Forvis Mazars in the Netherlands

Global state of cyber security

Quantifying cyber security value

Organisations are moving beyond mere technical metrics to assess cyber security effectiveness through business impact, looking at achievements like disruptions avoided and revenue enabled by strong security. This shift is key to securing funding and demonstrating the return on investment (ROI).

The cost concern: cyber security as investment, not expense

The proliferation of threats and the complexity of modern technology environments can make cyber security feel like an ever-expanding cost centre. However, leading organisations are reframing cyber security spending as a strategic investment.

Many organisations are realising the competitive advantage of solid cyber practices. Strong cyber security postures are an increasingly valuable differentiator in the market, particularly in B2B sectors where customers evaluate vendor security as part of their own risk management. There is a compliance element to this increased focus – customers need to think about their supply chains for the purposes of their own compliance – but customers also frequently cite high-profile incidents

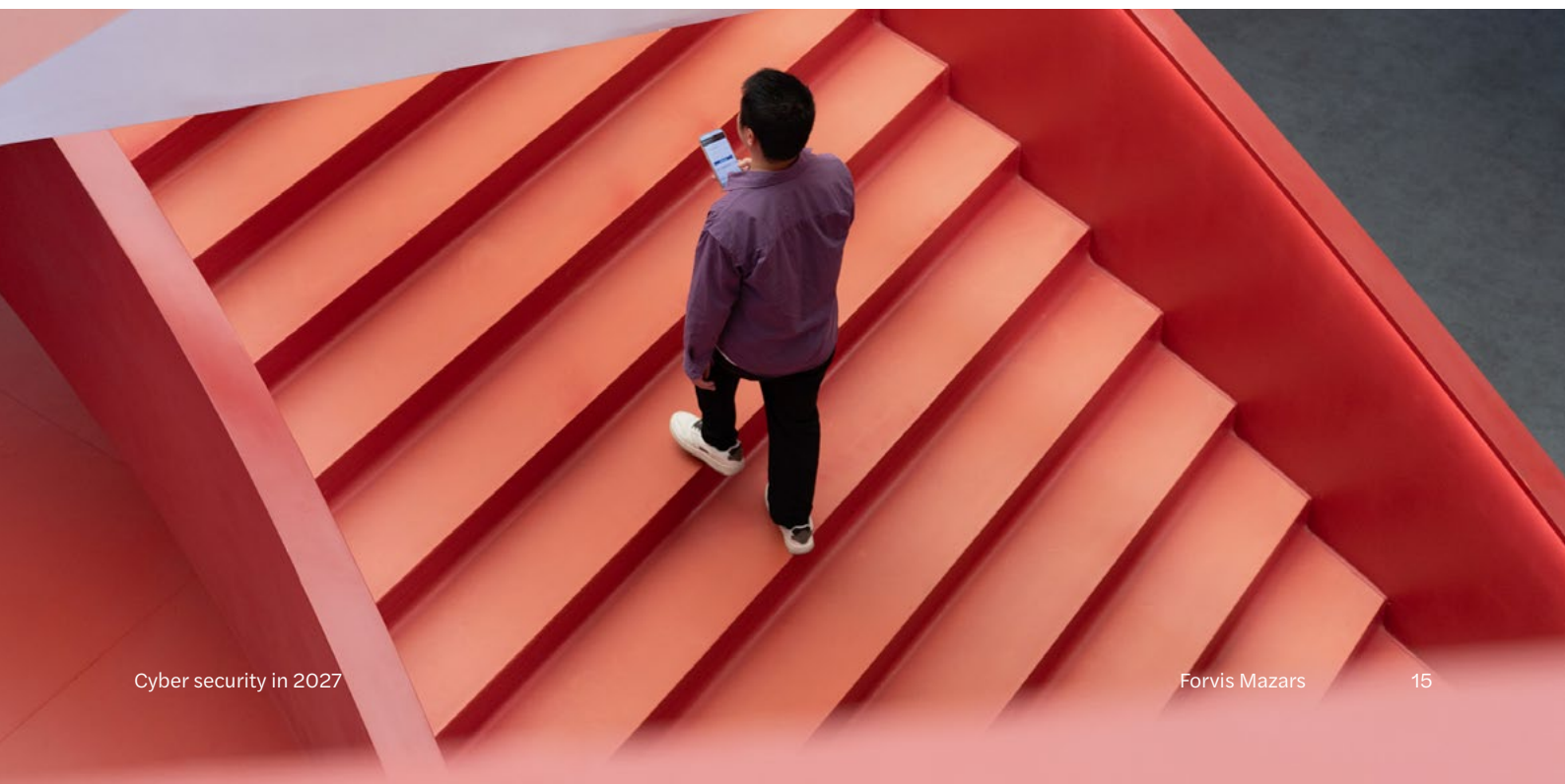
when raising cyber requirements, showing an increased market awareness of the potential impact of a disruption. Cyber teams that can quantify and communicate the value of this advantage can unlock unprecedented levels of buy-in.

“The age of cyber security as a necessary cost is ending, and the age of cyber security as a strategic differentiator has begun.”



Jeffrey de Bruijn
Director,
Forvis Mazars in the Netherlands

Of course, cyber security is important to more than just customers. Cyber insurance providers are naturally more concerned than ever with what measures are in place, and financing institutions are increasingly factoring cyber security readiness into their risk assessments. Both insurance and financing offer quantifiable incentive for strong security programmes.



Global state of cyber security

Quantifying cyber security value



Measuring what matters

Leading organisations are moving beyond traditional security metrics to focus on measuring success in ways that directly relate to business outcomes and stakeholder value. This includes:

- **Recovery time objectives:** how quickly can normal operations be restored after an incident?
- **Business impact metrics:** what is the actual cost of security incidents in terms of revenue, customer relationships and competitive position?
- **Stakeholder confidence measures:** how do security capabilities affect customer, investor and partner confidence?
- **Innovation enablement:** how effectively does the security programme support business innovation?



Optimising the ROI of cyber security spend

Organisations that invest in proactive cyber security measures consistently demonstrate better outcomes than those that take reactive approaches. Yet with resources limited in even the largest organisations, the following investment focuses can help optimise for ROI and reduce risk:

- **Risk-based prioritisation:** focus both human resource and capital on protecting the most critical assets rather than attempting to secure everything equally.
- **Security by Design:** build security requirements into systems and processes from the beginning, rather than trying to add them later.
- **Integrated approaches:** look for security solutions that address multiple requirements simultaneously, reducing the need for point solutions.
- **Automation and efficiency:** invest in tools and processes that amplify human capabilities rather than simply adding more personnel, especially regarding continuous monitoring for ongoing visibility.
- **Employee education:** implement regular training and awareness programmes that reduce the likelihood of human error-related incidents and social engineering vulnerability.
- **Incident response preparation:** develop and regularly test incident response capabilities in full before they are needed.
- **Shared services:** consider shared or virtual cyber security services where appropriate, particularly for specialised expertise that does not require full-time internal resources.

Global state of cyber security

How can businesses improve their cyber resilience in 2027?

Looking ahead to 2027 and beyond, cyber resilience will mean more than preventing attacks. Organisations will need to show that they can anticipate disruption, keep critical operations running and adapt as threats change.

For one, Security by Design will continue to transition from a best practice to a business necessity. More consistently, organisations will be expected to demonstrate to customers, regulatory bodies and insurers that security considerations are integral to their system design and business processes.

This approach will be particularly critical where AI is involved, and the security implications of design decisions may not become apparent until systems are already in production. Organisations that fail to implement Security by Design principles may find themselves at significant disadvantages in security effectiveness, market reception and regulatory compliance.

The pace of technological change will also necessitate governance frameworks that can adapt quickly to new challenges while maintaining consistent core principles. Resilient organisations will develop governance structures that can work seamlessly across organisational boundaries and technical systems, learn continuously and anticipate emerging threats and opportunities.

As the tech landscape is shaped by unstoppable seismic shifts, resilient organisations are building capabilities that can weather change regardless of any specific technology models, platforms or tools. This means adopting an ongoing risk-based approach to threat assessment, creating tool and vendor agnostic architectures where possible and focusing on skills-based workforce development.

Ecosystem-wide risk management

Resilience in 2027 will require businesses to think beyond their own boundaries to consider the security of the entire business ecosystem. This includes not only traditional supply chain partners but also technology vendors, service providers and even competitors in shared infrastructure arrangements.

Key components of ecosystem-wide risk management include:

- **Shared threat intelligence:** collaborating with partners to identify and respond to threats that affect multiple organisations or entities.
- **Coordinated incident response:** developing response capabilities that can function across organisational boundaries.
- **Standardised risk assessment:** using common frameworks, metrics and taxonomy to evaluate and communicate risk across the ecosystem.
- **Collective defence capabilities:** participating in industry-wide initiatives to develop shared defensive capabilities.

“The most resilient organisations focus on governance strategies that allow them to scale rapidly. They need to be able to accommodate new technologies and business models without requiring complete framework overhauls.”



Paul Truitt
Principal, Cyber Security Practice
Leader, Forvis Mazars in the U.S.

Innovation built on security

As we look towards 2027 and beyond, the organisations that will succeed are those that start preparing today by building the capabilities, partnerships and governance structures to navigate an increasingly complex and rapidly evolving threat landscape while capitalising on the tremendous opportunities that emerging technologies present.

“The future of cyber security is not about choosing between security and innovation, it is about achieving both simultaneously. This means thoughtful planning, strategic investment and collaborative approaches that recognise cyber security as a shared responsibility.”



Jan Matto
Senior Advisor Digital Trust,
Former Partner, Forvis Mazars
in the Netherlands

The path forward requires several key commitments:

Embrace change while maintaining principles: technology will continue to evolve, but fundamental security principles should remain constant. Organisations should strive to be agile enough to adapt to new technologies and at the same time stay consistent enough to maintain strong security postures.

Invest in people and partnerships: the cyber security challenges of 2027 and beyond will stretch many organisations' internal capabilities, making strategic partnerships and continuous workforce development increasingly important.

Measure business impact: security programmes should demonstrate their value in business terms, not just technical metrics. This requires cyber security professionals to develop business acumen alongside technical expertise.

Think ecosystem-wide: individual organisations cannot achieve true resilience in isolation. Cyber security needs to be approached as a shared challenge requiring coordinated responses.



Contacts

George Lagarias

Chief Economist,
Forvis Mazars
george.lagarias@mazars.co.uk

Jan Matto

Senior Advisor Digital Trust, Former Partner,
Forvis Mazars in the Netherlands
jan.matto@forvismazars.com

Wadi Mseddi

Group Head of Cyber Security Consulting,
Forvis Mazars
wadi.mseddi@forvismazars.com

Jeffrey de Bruijn

Director,
Forvis Mazars in the Netherlands
jeffrey.debruijn@forvismazars.com

Ali-Sultan Kirgizbaev

Partner, Head of Data & AI Centre of Excellence,
Forvis Mazars
ali-sultan.kirgizbaev@forvismazars.com

Paul Truitt

Principal, Cyber Security Practice Leader,
Forvis Mazars in the U.S.
paul.truitt@us.forvismazars.com

Anton Yunussov

Head of Cyber Security Practice,
Forvis Mazars in the UK
anton.yunussov@mazars.co.uk

Sean Andrews

Manager, IT Risk & Compliance,
Forvis Mazars in the U.S.
sean.andrews@us.forvismazars.com

Christopher Hock

Director,
Forvis Mazars in Germany
christopher.hock@forvismazars.com

Tom Tollerton

Principal, CMMC Practice Lead,
Forvis Mazars in the U.S.
tom.tollerton@us.forvismazars.com

Jakob Haesler

Global Head of Consulting,
Forvis Mazars
jakob.haesler@forvismazars.com

Forvis Mazars Group SC is an independent member of Forvis Mazars Global Limited, a leading professional services network. Operating as an internationally integrated partnership in over 100 countries and territories, Forvis Mazars Group specialises in audit, tax and advisory services. The partnership draws on the expertise and cultural understanding of over 40,000 professionals across the globe to assist clients of all sizes at every stage in their development.

© October 2026

forvismazars.com

forv/s
mazars