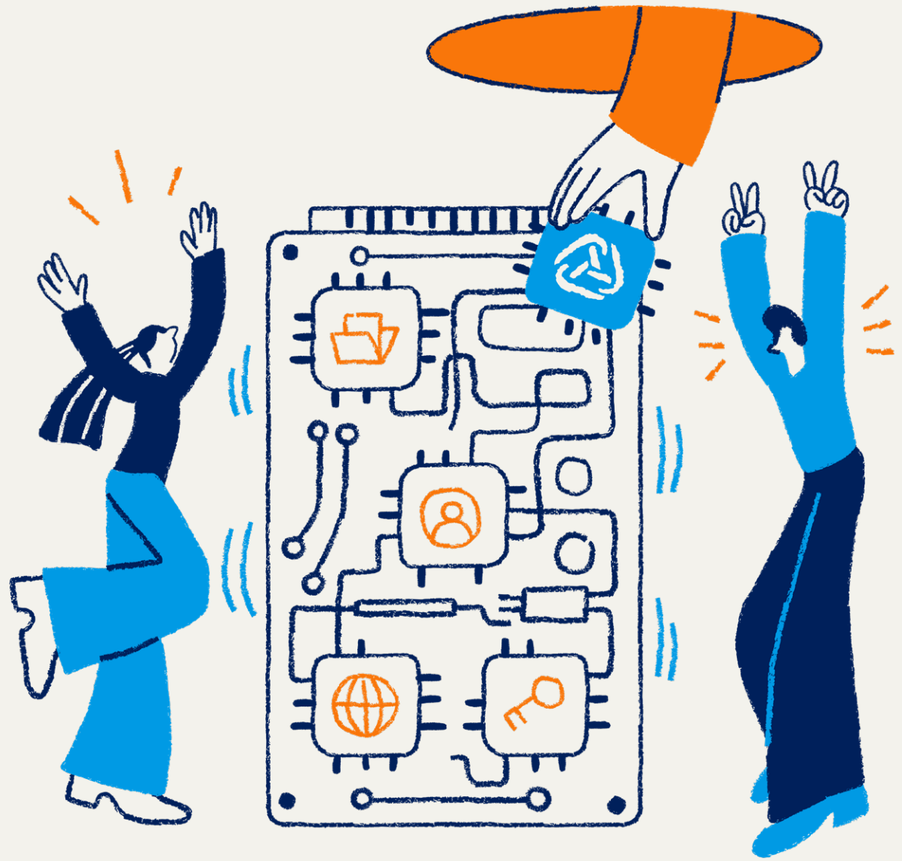
QBE Insurance

The new anatomy of a cyber crisis



At the heart of it

How dependency, concentration and control failures turn cyber incidents into operational disruption

Three key takeaways

1. Cyber resilience depends on managing critical business dependencies as rigorously as cyber security control.
2. Familiar weaknesses are turning cyber incidents into prolonged business disruption.
3. Recovery capacity is a resilience risk in its own right.

Executive summary

Cyber resilience now depends on managing business dependencies. Organisations have become heavily dependent on interconnected digital ecosystems, cloud infrastructure and software providers that are essential but often sit outside their direct control. As a result, an organisation's resilience is increasingly determined by its ability to withstand and recover from failures across complex networks of suppliers and service providers.

Three shifts shaping cyber risk

1. **Speed:** Attackers are moving from initial access to exploitation in a matter of minutes rather than days. This leaves organisations with less time to detect and respond to incidents.
2. **Concentration** has deepened as critical sectors rely on a relatively small number of cloud providers, software platforms and service providers. A disruption affecting one major provider can impact many industries and jurisdictions.
3. **Convergence** between information technology, operational technology and connected devices is expanding the potential consequences of cyber incidents, potentially disrupting physical operations and essential services.

Geopolitical tensions are driving increased cyber activity

Conflicts in Europe and the Middle East have been accompanied by an increase in disruptive cyber operations targeting critical infrastructure, public services and major commercial organisations.

Hybrid warfare increasingly blurs the boundary between geopolitical conflict and criminal behaviour. Healthcare, transport, logistics, technology and other strategically important sectors have become prominent targets. For example, in late 2025 Russia staged a large-scale disruptive attack against the Polish energy sector in the middle of winter.

Not all disruption is malicious

The October 2025 Amazon Web Services outage and November 2025 Cloudflare outage degraded banking, retail, transport and public-service platforms across multiple markets at the same time, in each case because a fault in one shared dependency propagated to everything running on top of it. Systemic resilience matters regardless of whether disruption comes from criminals or infrastructure failure.

Governments are responding to the threat

Governments and regulators are taking action to improve supply chain security, operational resilience, incident reporting and recovery planning. For example, the EU, UK and Canada have all recently legislated to strengthen requirements for supplier oversight, tested recovery and incident reporting.

At the same time, concerns about digital sovereignty, technology dependence and strategic competition are driving new restrictions on technology, data and cross-border digital activity.



The SME challenge

There is an important challenge for governments, insurers and the cyber-security sector around SMEs. Large organisations face regulatory and commercial pressure to demonstrate cyber resilience, but SMEs often have fewer internal resources while depending on many of the same technologies and interconnected supply chains.

Greater awareness and practical support are very important. Cyber resilience does not necessarily demand expensive technology. Sensible measures such as multi-factor authentication and effective backups can significantly help firms withstand an incident.

For larger organisations this is also a supply-chain issue. Helping smaller suppliers improve their resilience can ultimately protect the continuity of the businesses that depend upon them.

Five recommendations to strengthen resilience

1. **Proactive security:** Enforce MFA and patch vulnerabilities
2. **Governance and ownership:** Agree risk appetite at a senior level and name a single owner
3. **Dependency mapping:** Map critical services to providers and establish ways to recover
4. **Testing and exercising:** Test recovery and conduct exercises with executives
5. **Preparedness and response:** Secure forensic, legal and communications capacity in advance and rehearse decision-making

Cyber insurance as a service

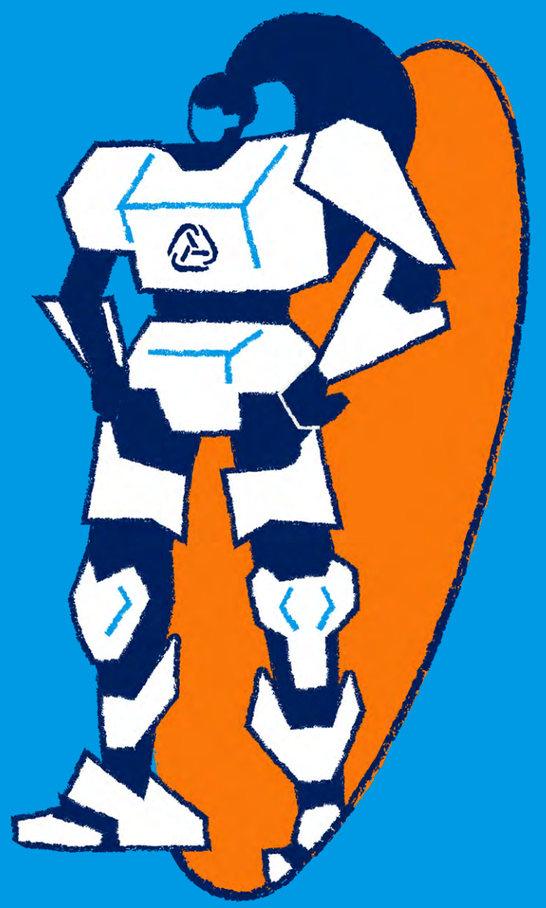
Businesses should not view cyber insurance as a strictly financial mechanism that responds after a loss. It provides access to expertise before, during and after an incident. Brokers and insurers can help organisations understand their exposures, identify areas where resilience planning would be valuable, and make better use of the specialist services available to them.

Introduction: when dependency outpaces control

As the number of potential entry points grows, cyber resilience is becoming increasingly intertwined with wider business resilience. With organisations increasingly dependent on interconnected digital systems, effective cyber security must extend beyond preventing attacks to understanding how disruption can spread through the business and how quickly critical operations can recover.

Most organisations understand that malicious cyber actors can cause significant business disruption. What is less well understood is why the same categories of attack now have a greater impact on targeted organisations than they did three years ago. One recent industry survey suggests that ransomware now costs the average affected organisation 24 days of operational downtime as a direct result of the attack,[1] while another estimate notes that broader recovery time for serious incidents averages as long as three to six months.[2 3]

The answer lies not just in expanding attacker capabilities, but also in core changes in the target environment that undermine defences and expand attack surfaces. The cyber threat to business continuity is increasingly defined by the extent to which organisations now depend on digital systems they neither fully control nor can operate without. It's also contingent on whether they have identified these dependencies and whether they have planned proportionately for disruption.



1 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026
2 https://www.accenture.com/en/insights/security/redefining-cyber-resilience
3 Downtime refers to system, network or application outages from a cyber incident. Recovery refers to the process of restoring impacting systems to a secure and working state following an incident.

Three shifts have combined to exacerbate disruption and widen the gap between dependency on and control over technologies:

Speed

Recent years have seen attacker timelines be compressed significantly, shrinking the window in which defenders can detect and contain attacks.

> "Threat actors can now move [...] to exploitation within only 30 minutes"

This change is likely in large part a result of the increasing availability of frontier AI tools and platforms. For example, a recent investigation found that an AI-enabled campaign conducted a scaled, co-ordinated attack that would have taken a human operator around two weeks to stage in less than ten hours,[4] and other reports indicate that threat actors can now move from initial access to exploitation within only 30 minutes, down from about 100 minutes in 2021.[5]

Concentration

Across sectors and geographies, digitalisation initiatives have encouraged the concentration of systems and functions into joint infrastructure, with the aim of streamlining and simplifying digital company assets. For example, AWS, Azure and Google Cloud accounted for almost two-thirds of enterprise cloud network spending in 2025.[6] As the speed of digitalisation and interoperability is prioritised over controls, critical services increasingly rely on a small number of cloud providers, Software-as-a-Service (SaaS) suites, identity platforms and managed service providers (MSPs), raising the potential for disruption in one critical node to cascade across businesses and sectors.

> "Digitalisation initiatives have encouraged the concentration of systems"

Convergence

IT, operational technology (OT) and Internet of Things (IoT) estates are merging, and identity is consolidating onto single providers, so a compromise can now cross domains that were previously separate.[7]

The result is that common control failures – a missing multi-factor authentication (MFA) prompt, an unpatched legacy server on a flat network – can cascade further and faster across the organisation. Notably, 90% of breaches analysed in recent research can be traced back to preventable gaps such as limited system visibility, inconsistent controls and excessive identity trust.

Resilience is failing where dependency has outpaced control; concentration and convergence exacerbate the scale and severity of the disruption that follows. Building cyber resilience requires organisations to account for both.

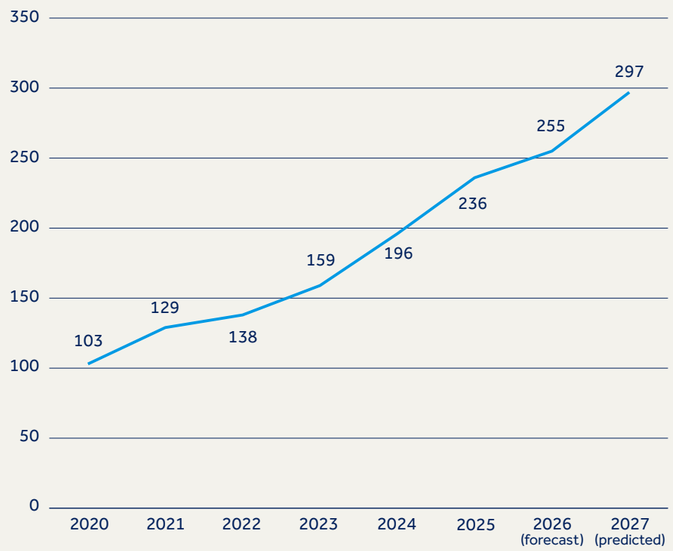
4 https://unit42.paloaltonetworks.com/ai-assisted-cyber-attack-inside-a-unit-42-investigation/
5 https://www.crowdstrike.com/en-us/press-releases/2026-crowdstrike-global-threat-report/
6 Synergy Research Group: AWS, Microsoft Azure and Google Cloud accounted for 63% of enterprise spending on cloud infrastructure services in Q3 2025. https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher
7 https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

Parallel challenges: disruptive intent, disruptive impact

Across the 14 QBE markets examined (see Scope and notes), disruptive incidents have risen every year since 2023 and are forecast to rise again in 2027.[9] What has changed is not only the volume but the average impact of successful attacks: where incidents typically caused a few days of disruption three years ago, disruption today is more likely to be prolonged because far more of the business depends on the systems that are affected.

Three drivers stand behind the trajectory: a mature criminal ecosystem that has professionalised access, tooling and negotiation; geopolitical fragmentation and hybrid activity that blur the line between state and criminal action; and the industrialisation of AI, which is likely contributing to compressed attacker timelines and making it easier for actors to stage convincing social engineering attacks. For example, researchers have suggested that AI-generated and automated personalised phishing emails have a 54% click-through rate. This is on par with personalised, human-generated phishing – which require more time and effort on the part of the attacker – but significantly higher than human-crafted, generic attempts that achieved a 12% click through rate.[10]

Figure 1: Number of strategically significant disruptive cyber incidents (2020-27)[11]



Source: Control Risks. See Scope and notes for regions, data methodology and limitations

"Cyber attacks do not simply compromise information; they stop organisations operating and cost millions on average.[8] In almost every case we respond to, the decisive factor is not how sophisticated the intrusion was, but how much of the business depended on the system that went down and how well the business had planned and prepared for disruption of that system."

Head of Cyber Threat Intelligence,
Digital Risks, Control Risks

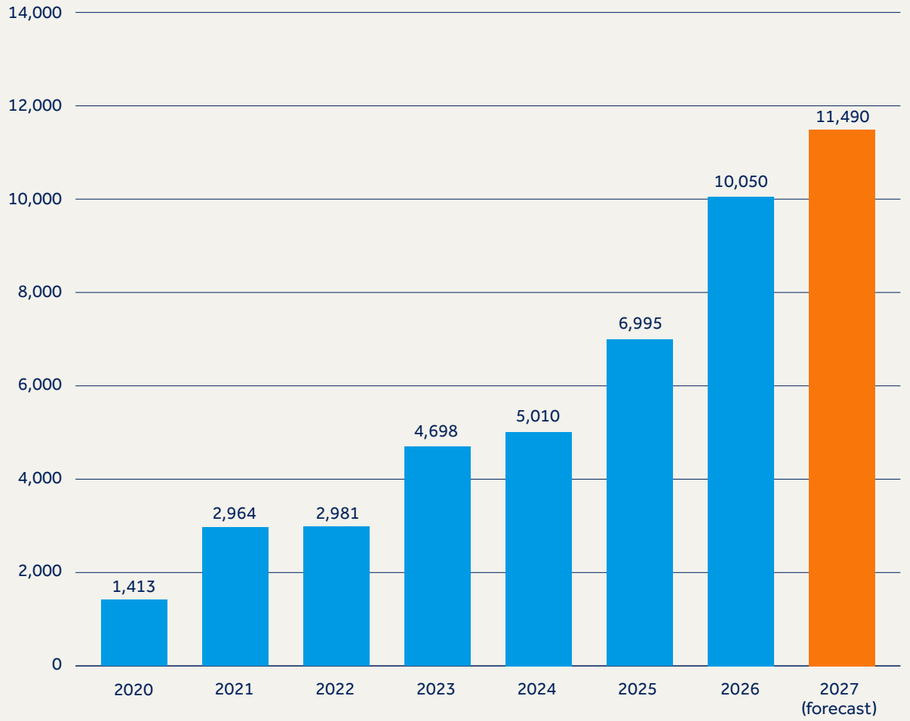
8 For example, IBM's Cost of Data Breach 2026 report indicates that the average breach costs victims USD $4.99 million, https://www.ibm.com/reports/data-breach
9 The aggregate number across the 14 markets
10 https://www.researchgate.net/publication/386374220_Evaluating_Large_Language_Models'_Capability_to_Launch_Fully_Automated_Spear_Phishing_Campaigns_Validated_on_Human_Subjects
11 This data is based on a curated set of incidents that fulfil one or more of several criteria, including the type of organisation targeted, the threat actor, the nature of the attack and objectives, and the impact.

Criminal extortion still dominates

Ransomware and data leak extortion remain among the most financially costly and potentially disruptive cyber threats facing organisations. In seeking to maximise disruptive impact, extortion actors increasingly prioritise known third-party vendors where disruption can reverberate across multiple customers and intensify pressure during extortion negotiations. Large corporations in manufacturing, retail, professional services and IT are regular targets of disruptive cybercriminal operations, with actors exploiting interconnected supply chains. For example, the 2024 ransomware and data leak extortion attack on Change Healthcare, a major healthcare payment processor in the US, has been estimated to have caused over USD $2 billion in direct costs and indirect damages.[12]

According to Control Risks' research, the number of victim organisations named on ransomware data leak sites increased by 611% between 2020 and 2026 and is forecast to increase by 14% in 2027.

Figure 2: Number of victim organisations named on ransomware data leak sites globally (2020-27)



Source: Control Risks' incident and intelligence data. See Scope and notes for regions, data methodology and limitations

12 https://hyperproof.io/resource/understanding-the-change-healthcare-breach/

But geopolitical frictions exacerbate the challenge

Geopolitical escalation in Europe and the Middle East has coincided with an increase in hybrid operations, including disruptive cyber operations. Activities observed in 2025 and 2026 have included disruptive attacks on critical infrastructure and high-profile brands staged by state actors like Russia and Iran. Across the 14 QBE markets in scope, such geopolitical drivers will likely be sustained in the medium to long term. This is likely to be coupled with short-term spikes in activity linked to scheduled events, such as the US midterms in November 2026 and the French elections in 2027, in line with the electoral interference patterns evident for at least a decade. As a result, businesses operating in these jurisdictions will continue to face threats to digital resilience.

> "Russia in late 2025 staged a large-scale disruptive attack against the Polish energy sector in the middle of winter"

Even as their disruptive intent has grown, states continue to seek to evade attribution, expanding their reliance on cybercriminal and cyber activist groups as a deniable way to cause disruption to adversary states. Although most of these groups sit outside its direct control of the state, states can encourage, incentivise or directly task such groups to conduct operations that align with state interests. For example, repeated warnings and punitive measures by European countries in 2026 demonstrate that Russia has significantly increased its use of Russia-based cybercriminal ecosystem as proxies to disrupt public and private entities in critical sectors like healthcare, transport and logistics and IT vendors.[13] While such groups remain primarily financially motivated, their disruptive impact serves strategic objectives within broader hybrid warfare campaigns.

Although individual businesses may not be the primary targets of geopolitically motivated disruptive attacks, incidents impacting key infrastructure suppliers, including the energy sector or critical IT vendors, are likely to cause downstream impact. For example, Russia in late 2025 staged a large-scale disruptive attack against the Polish energy sector in the middle of winter, underscoring its intent to use cyber operations to directly impact civilian life. Such high-impact incidents have historically been unusual, but are likely to become more commonplace, driven by both disruptive intent and the interconnected nature of the targeted systems. Similar threats will also continue to arise from cybercriminal and cyber activist proxy actors, whose capabilities are expanding through state actor assistance and the emergence of frontier AI.

13 https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/ | https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions | https://www.lovguiden.dk/en/det-offentlige/eu-udenrigstjenesten/2026-07-21-eu-advarer-fn-om-ruslands-cyberproxyer-og-ransomware-mod-sundhedssektoren | https://www.rbb24.de/politik/beitrag/2026/02/krankenhaeuser-berlin-hybride-bedrohungen-russland-cyberangriffe.html | https://therecord.media/ransomware-gangs-advancing-moscow-geopolitical-interests-warns-romania

Geopolitical fragmentation shapes resilience planning

Geopolitical friction has also driven regulatory changes, with policymakers focusing on digital sovereignty, technology restrictions and trade limitations. This includes the AI sector, where the United States and China continue their competition for global market and technological leadership. As policy changes continue to impact data privacy agreements, localisation requirements and technology availability, businesses are increasingly having to incorporate regulatory limitations and policy shifts in resiliency planning, for example when looking at optional providers for redundancy and broader compliance challenges that could arise in a crisis scenario.

With systemic disruptive threats likely to stay, operational resilience will come down to a combination of business preparedness, third-party risk and national frameworks.

Figure 3: Threat and readiness consideration across the 14 markets in scope

Markets	Geopolitical drivers of disruptive threats[14]	Readiness consideration[15]
Nordics, Germany, the Netherlands, France, the UK	State-aligned and cyber activist disruption tied to Russia-NATO friction, including against critical infrastructure	Mature national frameworks, but operational technology (OT) and critical infrastructure exposure concentrated in a few operators
The US and Canada	High volume of Iran-linked retaliatory disruptive attacks linked to US involvement in Middle East	Deep response and recovery market, but capacity is shared
Australia, New Zealand, Singapore, Hong Kong	Rising state-linked activity and alignment pressure between Washington and Beijing	Regulatory expectation rising faster than in-house response capability in several markets
Spain and Italy	Pro-Russia cyber activist activity tracking European policy positions, with Italy a regular target of low-level cyber disruption	Large supplier bases of smaller firms with uneven security maturity

Source: Control Risks' intelligence analysis. See Scope and notes for data methodology and limitations

14 This summary is based on Control Risks' data, evidence and assessment of the key geopolitical drivers of disruptive cyber threats in these locations.
15 This summary is based on Control Risks' assessment and third-party information on key readiness considerations in these locations, such as national-level resilience and preparedness frameworks, maturity of cyber security market and concentration/availability of providers among other factors.

Infrastructure failures without an attacker

Not all disruption is malicious. The October 2025 Amazon Web Services (AWS) outage[16] and November 2025 Cloudflare outage[17] degraded banking, retail, transport and public-service platforms across multiple markets at the same time, in each case because a fault in one shared dependency propagated to everything running on top of it. Neither event involved an adversary, and that is precisely what makes them instructive: they show that concentration risk crystallises on its own, with no one choosing a target. Even for an organisation holding no direct contract with either provider, the practical consequence could be the same: its suppliers were affected, and its recovery timeline was set by someone else.



16 Ookla/Downdetector analysis of the AWS US-EAST-1 disruption of 20 October 2025: more than 17m user reports across over 60 countries and more than 3,500 companies, with core impact lasting approximately 15 hours. https://www.ookla.com/articles/aws-outage-q4-2025
17 Cloudflare outage of 18 November 2025: an internal configuration fault degraded proxy and CDN services globally for approximately 3.5 hours, affecting a substantial share of global internet traffic. https://blog.cloudflare.com/18-november-2025-outage/

Concentration risks and supplier crunch set the odds

Figure 4: Technology dependencies

Technology dependency	Where it stands	Why it matters
Cloud	AWS, Azure and Google Cloud account for nearly two-thirds of enterprise cloud infrastructure spending.[18]	One provider failing creates correlated, not isolated, exposure across sectors and markets.
Third-parties	The percentage of breaches involving a third party doubled year-on-year in 2025, from 15% to 30%.[19]	The supplier, not the perimeter, is now the fastest-growing route in.
Identity	Access consolidating onto single providers spanning IT, OT and SaaS estates.	One compromise now crosses domains that were previously separate.
AI	Adoption concentrated on a small number of models, often without basic access controls; reported 77% of companies say AI adoption is outpacing controls.[20]	A new dependency is being embedded faster than it is being governed.

Source: Control Risks analysis and third-party data

The exposures examined here sit outside any single organisation's control, yet they determine how far a failure travels and how long recovery takes. Concentration onto shared cloud, SaaS, identity and MSPs means a fault or compromise at one provider may impact simultaneously every organisation that depends on it, and every organisation whose suppliers depend on it. Severe disruption therefore no longer requires an organisation to be the intended target or, in the case of an infrastructure outage, for there to be any target at all. For many organisations this is the least-mapped part of the risk picture, because it falls between security, procurement and business continuity, and no single function owns it.

This presents structural challenges that cannot be mitigated fully through contractual assurances or technical redundancy. Reliance on a narrow group of technology providers and platforms creates interdependencies that extend beyond conventional supplier risk. Modern cloud ecosystems can rely heavily on a single provider to underpin an entire spectrum of essential services, creating conditions where a single point of failure can trigger multi-service disruption across an organisation. This concentration risk is being amplified by the adoption of AI, as AI concentration mirrors and expands existing cloud and technology dependencies as many of the same companies sit across these services. At the same time, these concentration risks cannot be fully mitigated without trade-offs, whether capability, interoperability or security.

Critical technology vendors are often assumed to be too important to fail, leading many organisations to overlook their resilience. But incidents such as the 2025 outages of AWS and Cloudflare demonstrate that no technology is fail-safe. As a result, businesses (and key functions within businesses) inherit risks when they have not also built in redundancy measures and resiliency planning for when business critical systems managed by others are unavailable.

18 Synergy Research Group: AWS, Microsoft Azure and Google Cloud accounted for 63% of enterprise spending on cloud infrastructure services in Q3 2025. https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher
19 https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf
20 https://newsroom.ibm.com/2026-06-08-new-ibm-study-finds-cios-and-ctos-face-growing-ai-control-gap-as-enterprise-deployment-scales

Case study: when downtime becomes the loss

The 2025 ransomware attack against a UK-based retailer carried an estimated GBP £300 million impact on operating profit and led to online orders being suspended for 46 days, with full recovery running into 2026.[21] The 2023 compromise of US-based consumer goods manufacturer Clorox is estimated to have cause the company some USD $380 million in damages, with around USD $50 million in remedial costs and the rest linked to inability to ship products to customers.[22]
In both cases, the initial vector came through the supply chain but resulted in significant operational downtime following the breach, demonstrating the potential impact of wider supply chain dependencies.

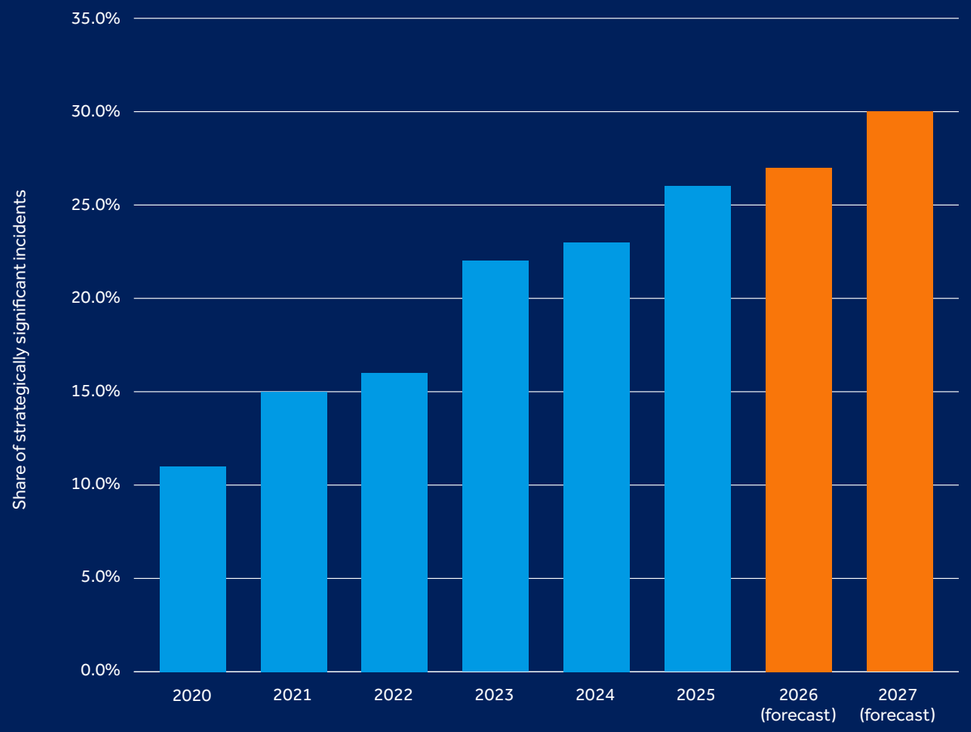
Control Risks has also responded to cases in the past two years in which affected companies were dissolved or sold for nominal sums in the aftermath of an attack. This is also supported by external statistics, which show that 60% of small companies targeted in cyber attacks are forced to shut down operations within 6 months of the incident.[23] The determining factor was not the sophistication of the intrusion but how long the business could not operate, with downtime in 2026 costing organisations an average of USD $15,000 per minute.[24]



21 Marks and Spencer Group plc disclosures and contemporaneous reporting, 2025-26: an estimated GBP 300m impact on FY2025/26 operating profit; online orders suspended from 22 April to 10 June 2025. https://www.bbc.com/news/articles/c0el31nqnpvo
22 The Clorox Company v. Cognizant Technology Solutions, Alameda County Superior Court, July 2025: USD £380 million claimed, comprising approximately USD $49 million in remediation costs and business interruption losses arising from the August 2023 attack. https://www.reuters.com/legal/government/clorox-accuses-it-provider-lawsuit-giving-hackers-employee-passwords-2025-07-22/
23 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026
24 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026

The supplier crunch: exposure runs deeper than the contract

Figure 5: IT companies targeted as a proportion of all strategically significant incidents (2020-2027 forecast)



Source: Control Risks analysis and third-party market data. See Scope and notes for regions, data methodology and limitations

Platform concentration is at least visible. What sits beneath it is not. Exposure extends past direct suppliers to their subcontractors and to shared software components that few organisations map, let alone monitor, and it determines recovery as much as it determines compromise:

- **Single points of failure:** Critical services may rest on one cloud region, one SaaS platform or one MSP, often without a tested alternative or a contractual right to recovery priority.
- **Extended supply-chain dependency:** A supplier's network of suppliers are rarely mapped, so the organisation cannot answer a simple question: who else has to be working, for us to keep working?
- **Recovery dependency:** Restoration timelines are often reliant on factors outside the organisation, including vendor patching, a provider's own recovery timeline or third-party backup platform.
- **Nature of backups:** Regular back-up testing can shorten downtime by an average of 15 days.[25] However, industry research indicates that 94% of ransomware victims run backup systems jointly with production environments targeted by attackers, potentially compromising recovery options when they are needed most.[26]

25 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026
26 https://fenix24.com/2026-state-of-recoverability-report/

Sector convergence turns one vendor failure into a sector event

Sectors are converging on the same specialist platforms, whether a dominant SaaS suite, a common OT vendor or a shared MSP, often because certification requirements, regulation or client expectation narrow the field of acceptable suppliers. A single vendor failure can therefore disrupt competing organisations at the same moment, and a sector-wide outage removes the option of turning to a peer for capacity.

> "Regulators have begun to treat this as a systemic problem"

Regulators have begun to treat this as a systemic problem rather than a procurement one: The EU's Network and Information Security Directive 2 (NIS2) and Digital Operational Resilience Act (DORA),[27] the pending update to the UK's Cyber Security and Resilience (Network and Information Systems) Bill and Canada's Critical Cyber Systems Protection Act all push requirements for supplier oversight, tested continuity and incident reporting down through supply chains. Organisations in scope, and the far larger number that supply them, should expect concentration and recovery dependency to become a matter of demonstrable compliance rather than internal judgement.



27 As of July 2026, France, Spain and the Netherlands (three of the 14 QBE markets) had not notified full transposition, and the European Commission referred them (along with Ireland) to the Court of Justice. https://digital-strategy.ec.europa.eu/en/news/commission-refers-ireland-spain-france-and-netherlands-court-justice-failing-transpose-rules The Netherlands' Cyberbeveiligingswet subsequently came into force on 15 August 2026, implementing NIS2. https://www.nldigitalgovernment.nl/dossiers/nis2-directive-cyberbeveiligingswet-cbw/

When incidents become crises

The security failings that cause disruptive events are consistent across Control Risks' intelligence database of open source and response cases. Many of these failings are being exacerbated by expanding attack surfaces and increasing threat actor capabilities, including those enabled by AI.

Five recurring weaknesses turn incidents into crises



Identity, access and people
Absent or by-passable MFA, credential reuse and over-privileged accounts all expand attack surfaces. AI-enabled social engineering is making convincing lures easier to produce and scale, including those targeting senior, technical and core business staff (HR, legal, finance).



Unpatched and legacy systems
Most vulnerabilities exploited in 2025 were known issues for which fixes already existed.[28] In 2026, the emergence of AI-enabled vulnerability discovery has significantly increased the volume of vulnerability disclosures,[29] making it more difficult for organisations to prioritise patching practises.



Poor segmentation
Flat IT or OT networks inherently let attackers move from a corporate foothold straight into operational systems, or across critical IT systems in an organisation. AI is now being leveraged to chain together security weaknesses that in the past would have limited the ability of attackers to traverse networks, making genuine data segmentation even more critical.



Third-party exposure
Suppliers, MSPs and software platforms are a significant initial access route, with threat actors even targeting suppliers' third-parties to gain access to highly attractive target environments.



Detection and response gaps
Limited monitoring of anomalous events and/or the ability to quickly block incidents, and business continuity and response plans that are untested or not mapped to the organisation's critical services. As AI enables threat actors to accelerate elements of the attack sequence, the impact of these gaps could be further exacerbated.

These failings share a pattern. In almost every case Control Risks responds to, the organisation did not spot the intrusion early enough, could not contain it once it began to spread, could not operate without the system it lost and had not adequately prepared for any of these scenarios.

28 Verizon, 2025 Data Breach Investigations Report: exploitation of vulnerabilities as an initial access vector rose 34% year on year and featured in 20% of breaches, predominantly known and patchable issues in edge devices and VPNs. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf
29 The CISA Common Vulnerabilities and Exposures (CVE) programme in September reported that CVE submissions in the first quarter of 2026 were one third higher than during the same period in 2025. Google's Threat Intelligence Group in September reported a doubling of vulnerability disclosure between January and August 2026. https://www.cisa.gov/sites/default/files/2026-09/cve-program-establishing-a-quality-era-framework-508c.pdf https://therecord.media/google-vulnerabilities-cyberattacks-ai

In Control Risks' experience, it is these shortcomings that separate a contained incident from a business crisis:

Figure 6: Why incidents become crises

The failure	What it looks like	Why the incident escalates
They could not see it	Partial monitoring coverage, alerts unreviewed outside working hours	Attackers can now move laterally in around 30 minutes;[30] undetected access enables full compromise
They could not contain it	Flat networks, shared credentials, standing privileged access	A corporate foothold reaches operational and production systems
They could not operate without it	Critical services never mapped to the systems and suppliers beneath them	Technical outage becomes lost trading; ransomware downtime now averages around 24 days[31]
They had not practised	Plans written but untested, and never exercised above the technical team	Executive decisions are taken for the first time under maximum pressure

Source: Control Risks' incident response casework.

30 https://www.crowdstrike.com/en-us/global-threat-report/
31 Coveware by Veeam quarterly ransomware reporting and associated industry analysis, 2025.

Business functions are attack surfaces of their own

Attackers do not target organisations at random. Even the most opportunistic of groups have strategies, preferences and routes of least resistance, and understand where and the easiest opportunities for compromise lie. They target the functions that hold access, money, data or trust, because these offer the fastest route to disruption and the greatest extortion leverage to impact the broader organisation.

In Control Risks' response casework, the functions listed are the most consistently targeted as an initial vector into organisations, and they are not always the functions organisations expect:



IT, security and privileged administrators: Credential theft and help-desk impersonation scale a single compromise enterprise-wide.



Finance, payroll and procurement: Payment authority makes these functions attractive targets for business email compromise, invoice fraud and deepfake-enabled payment diversion.



Operations, engineering and OT: Where digital disruption can become physical and downtime can carry significant operational costs.



Customer-facing and sales: Externally exposed and a bridge to customer data and systems.



Executive and board: Hold approval authority and are prime targets for impersonation.



HR and people: Hold personal data and manage inbound applications, creating exposure to tactics including fraudulent IT-worker infiltration.

Some roles face disproportionately high levels of targeting. Mergers and acquisitions (M&A) staff and those with roles closely related to deal making, divestments and investments are a critical target for both financially and commercially motivated threat actors.

Through Control Risks' research and work with private market clients, approximately 18% of the total number of ransomware and data leak victims had been involved in a public merger or acquisition in the past 12 months, indicating disproportionate targeting of organisations involved in public M&A activity. In private market organisations, M&A staff are frequently targeted by phishing and social engineering attempts more often than IT or internal finance teams. This trend correlates across markets, with M&A staff targeted disproportionately in other non-capital market sectors.

Business functions can increase exposure and resilience challenges in three key areas:

Direct targeting:
As discussed, threat actors target specific business functions within organisations using a range of social engineering techniques to enable system compromise, disruption, data theft or extortion.

Vulnerability management:
Gaps in identifying unapproved software, including unsanctioned AI tools, patching legacy systems and deploying security controls consistently across devices can create readily exploitable weaknesses.

Poor resilience planning:
Although systems and technologies are increasingly managed centrally, the differing uptime, dependency and redundancy requirements of individual business functions are often not always reflected in resilience planning, increasing the potential cost of disruption.

Five recommendations to strengthen operational resilience and reduce recovery time

Resilience is not a posture or a maturity score. In Control Risks' casework, organisations that recover quickly tend to have done the same small number of things, and none of them requires new technology. They require someone to own the question of what the organisation cannot operate without, and to keep answering it as that answer changes.

Figure 7: Five resilience activities that shape recovery time



1 **Proactive security**	Enforce MFA wherever technically possible, remove standing privileged access, patch known and exploited vulnerabilities first, and segment IT from OT so a corporate foothold cannot reach production.
2 **Governance and ownership**	Assess the risk profile, agree risk appetite with senior stakeholders and name a single owner for dependency and continuity. When this sits between security, procurement and business continuity, it is owned by no one.
3 **Dependency mapping**	Map critical services to the systems, providers and nth-party suppliers beneath them, identify when recovery requires third-party involvement, and agree workarounds and establish contractual recovery expectations, priorities and workable alternatives where possible.
4 **Testing and exercising**	Test recovery against the loss of a provider, not only the loss of a system, and exercise with executives as well as technical teams. An untested plan is an assumption, and assumptions fail first.
5 **Preparedness and response**	Secure forensic, legal and communications capacity in advance, rehearse decision-making thresholds and revisit the risk profile as the estate and supplier base change. Planning these decisions in advance reduces the number that must be made for the first time during a crisis, leading to quicker recovery and less disruption.

Source: Control Risks

Together, these five activities answer four questions every organisation should be able to answer with evidence.

- → Can it see an intrusion early enough to act on it?
- → Can it contain the intrusion before it reaches operational systems?
- → Can it keep delivering its most critical services while the affected system is unavailable?
- → And has it practised doing so, with executives as well as technical teams?

Organisations that can answer all four questions tend to recover more quickly. Those that cannot have less control over the duration and impact of disruption, particularly where recovery depends on third parties. That is what makes dependency a board-level question: it determines recovery time, the true cost of downtime and how much of the organisation's continuity is decided outside its own perimeter.

At the heart of underwriter insights



David Warr
Portfolio Manager

One of the clearest lessons from the cyber losses we see, is that the severity of an incident isn't necessarily determined by how sophisticated the attack was. Often, what matters more is what happens next. That might be how far disruption impacts through an organisation, which critical services become unavailable, how quickly they can be restored, or how dependent recovery is on third-parties. This changes the way we think, and how businesses should think, about cyber resilience.

Strong security controls will always be fundamental, but preventing every incident is not a realistic objective. Organisations also need to understand how they would continue operating when a critical system, supplier or technology platform is unavailable – and how much control they actually have over their own recovery timeline.

For underwriters, it's an important and valuable distinction. Two businesses with apparently similar cyber security controls can have very different exposures to loss. One may have mapped critical services, segmented networks, tested backups, identified alternative suppliers and rehearsed responses with senior leaders. Another may discover the critical dependencies only after an incident has occurred. The initial cyber event could be similar, but the subsequent business interruption may be very different.

This is particularly important as organisations become more dependent on a relatively small number of technology providers. Managed services, platforms and systems have created fantastic efficiencies, but they can also create some big common points of dependency.

Businesses must therefore look beyond conventional third-party risk management. Knowing who your direct suppliers are is no longer enough. Instead, make a note of that key question: who else needs to be working for us to keep working? The answer may include a supplier's cloud provider, software platform or other subcontractor; one with which your own organisation has no direct relationship at all. But – if that provider fails, recovery may run on someone else's timescale.

It's also why concentration risk matters. Individual businesses cannot individually diversify a market in which large numbers of organisations depend on the same critical providers. Regulators and governments have an important role in considering how systemic technology dependencies are identified and managed, alongside the responsibilities of individual organisations.

Recovery needs to be designed, not assumed

One of the most valuable exercises a business can undertake is to work backwards from its critical services.

What must keep operating? Which systems and suppliers enable it? How long could the business function without them? What are the alternatives? Who has the authority to make decisions when disruption occurs? Those questions should be answered before an incident, not during one.

Testing is equally important. An incident response plan may look comprehensive on paper but still include assumptions that have never been tested. We recommend that organisations also stress test for the loss of a provider, as well as of an internal system, and exercises should involve executive level decision-makers alongside cyber security and IT teams. Businesses should know and plan in advance when they would invoke business continuity arrangements, communicate with customers, engage specialist support or make other critical decisions.

The commitment to preparation can materially affect the scale of a loss. The objective doesn't stop at restoring technology, the focus should centre on preserving the ability to deliver the most important services while recovery takes place.

Don't overlook smaller businesses

There is also an important challenge for governments, insurers and the wider cyber-security sector around smaller and medium-sized businesses (SMEs). Large organisations face regulatory and commercial pressure to demonstrate cyber resilience, but SMEs often have fewer internal resources while depending on many of the same technologies and interconnected supply chains.

Greater awareness and practical support are very important. Cyber resilience does not necessarily demand sophisticated or expensive technology. Sensible measures such as multi-factor authentication (MFA), removing unnecessary privileged access, patching exploited vulnerabilities, maintaining effective backups and understanding critical supplier dependencies can significantly improve the ability to withstand an incident.

For larger organisations, this is also a supply-chain issue. Helping smaller suppliers improve their resilience can ultimately protect the continuity of the businesses that depend upon them.

Use the expertise around you

Finally, businesses should not view cyber insurance as a strictly financial mechanism, that responds after a loss. The insurance relationship can provide access to expertise before, during and after an incident. Brokers and insurers can help organisations understand their exposures, identify areas where resilience planning would be valuable, and make better use of the specialist services available to them.

In an incident, knowing in advance who to contact (forensic specialists, legal advisers, communications experts, response providers) can save valuable time in the early stages of a crisis.

Scope and notes

Markets in scope (14)

The analysis covers 14 markets in which QBE operates: the UK, Sweden, Denmark, France, Germany, Spain, Italy, the Netherlands, Canada, the US, Australia, New Zealand, Singapore and Hong Kong.

Period

2023-26, with a forward look to 2027.

Sources and method

The analysis draws on Control Risks' incident, intelligence and response data across the 14 markets in scope, supplemented by open-source reporting and third-party market data where cited. Figures for 2026 take the year-to-date numbers and then forecast to year close; 2027 figures are forecast based on average growth.

Data methodology

Control Risks' dataset is based on reporting curated for a corporate audience, typically large multinationals, and focuses on strategically significant incidents. This differs from providers that source data from endpoint detection and response tooling deployed across their own customer base, which will typically capture both large multinationals and smaller enterprises. Control Risks' data will not capture every incident an automated tool would, but it is a good representation of incidents affecting large corporates in the markets in scope.



For more information on this report,
visit **qbe.com/cyber**

QBE European Operations
30 Fenchurch Street
London EC3M 3BD
United Kingdom
+44 (0) 20 7105 4000

QBEeurope.com

This report was produced by QBE with Control Risks.

All products and services are provided by QBE Insurance Group Limited or its subsidiaries ("QBE") or by QBE's selected third party vendors and may be subject to additional terms and conditions, limitations and disclaimers [available on request]. Information and guidance provided by QBE is not intended to constitute any financial or professional advice tailored to your circumstances and may not have been prepared with detailed knowledge of your systems or the risks to your business, and does not cover all possible situations or actions necessary to respond to a cyber security incident. QBE does not make any guarantees regarding outcomes, such as reduced claim exposure or that a product or service will meet your unique needs. You are responsible for using your independent judgment to assess the advice provided and the suitability of any product and this does not replace the advice of legal counsel or cyber security professionals in preparing for, or responding to, a cyber security incident. QBE is not liable or responsible for services provided by its third party vendors. QBE and the chain links logo are registered trade marks of QBE Insurance Group Limited and third party marks are duly licensed. © 2026 QBE Insurance Group Limited.

QBE European Operations is a trading name of QBE UK Limited, QBE Underwriting Limited and QBE Europe SA/NV. QBE UK Limited and QBE Underwriting Limited are both authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority. QBE Europe SA/NV is authorised by the National Bank of Belgium under licence number 3093.

1475304/2611-UK

QBE Insurance