ECONOMIST ENTERPRISE

The cost of complacency: Why cyber resilience needs to be valued

Supported by rubrik

Ask most chief financial officers (CFOs) what a day of operational downtime would cost after a flood or a factory fire, and they will likely have an answer. Ask the same question about a cyber incident, and many won't. That uncertainty has a price: boards often treat cyber resilience as a cost centre even as AI increases the risk. Ninety-eight percent of organisations surveyed in recent Economist Enterprise research have reported an agent-related disruption, while nine in ten expect such incidents to become more frequent regardless of safeguards.[1] Failure to invest adequately in resilience is the single most expensive decision companies can make.

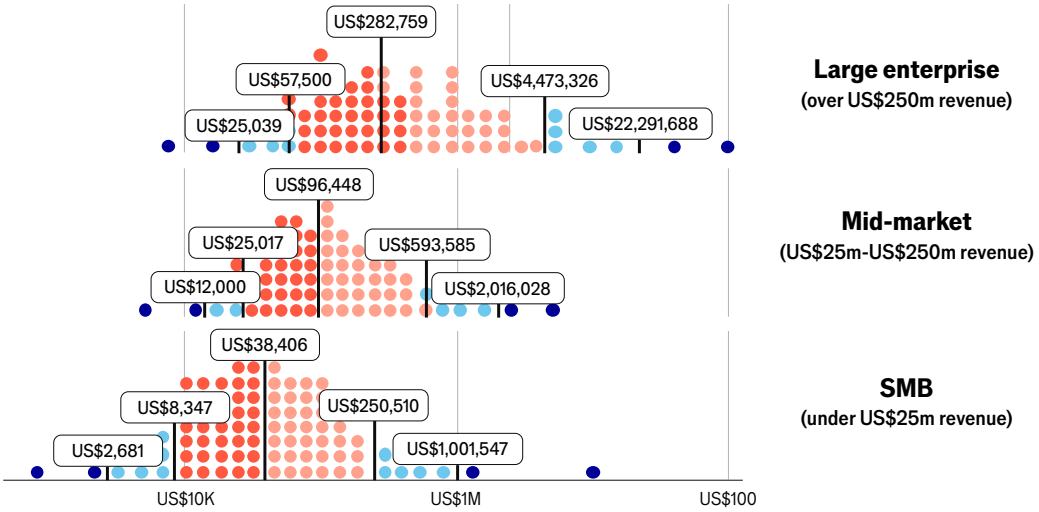
The unguarded crown jewels

Ever since the mid-90s, intangible assets — software, customer data, intellectual property, algorithms, brand — have accounted for most of US companies' market value, reaching 92% of S&P 500 market capitalisation. Yet investment in protecting those assets has long lagged behind the value they represent.[2]

While boards recognise the stakes, putting a dollar figure against exposure is complex. "The financial cost of a breach is a very open question," explains Ashish Khanna, managing director of global security services at Verizon. "It depends on the maturity of the company, how prepared they are and which industry [they operate within]."

The economic impact of an incident also varies widely depending on firm size. Figure 1 quantifies the frequency of these different cost impacts: each row shows the full spread of cyber-incident losses by company size, with warm-coloured dots marking the typical middle 80% of cases, green marking the unusual tails and blue marking the true outliers.

Figure 1: Cost clusters
Distribution of financial impact per cyber incident by company size (US$)



Note: Dot color reflects statistical confidence: orange/peach = 80% range, light blue = 80th-95th percentile, dark blue = outliers.
Source: Verizon[3]

> **"The cost isn't just brand, and it isn't just business disruption. There's actual physical work — human cost and systems cost. You're suddenly having to prioritise work, maybe slow down a product roadmap, features you were going to deliver. That's future revenue you're not capturing. There's the cost of human effort to mitigate and rebuild. And then there are the investigation costs, which can run into the millions of dollars. These costs can have a very long tail."**
>
> - **Ann Johnson**, executive vice president of security solutions at Mastercard

Typical losses scale with company size — US$38,000 for small firms, US$96,000 for the mid-market and US$283,000 for large enterprises, while the worst cases reach more than US$22m.[4]

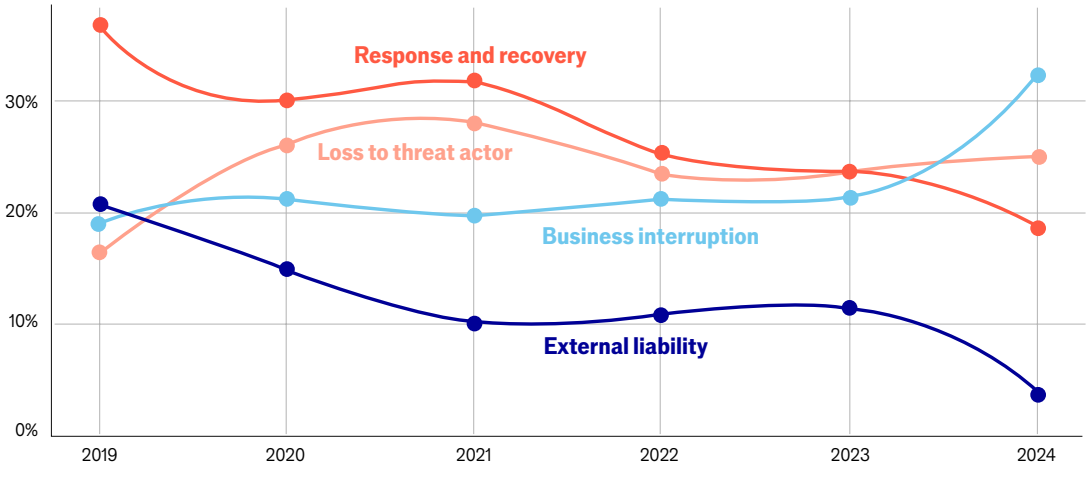
The costs don't end at the targeted company, either. The massive Jaguar Land Rover cyberattack in 2025 not only affected the company's finances but that of many of its suppliers, which is also the case in many similar large-scale cyberattacks across industries.

For every board and CEO, the urgent governance question is how to meaningfully calibrate resilience spend against the financial cost of inaction. In 2025, Gartner warned that over 40% of agentic AI projects could be cancelled by 2027 due to factors such as escalating costs, unclear business value and weak risk management. Another study by S&P Global found that the percentage of companies abandoning the majority of their AI initiatives before production surged from 17% to 42% year over year.[5] Organisations from Alibaba to the European Parliament have already halted agentic initiatives due to cybersecurity risks like unauthorised activities and data leaks.[6,7]

Counting the cost

Finance leaders might focus on the costs of ransom payments, but the operational cost of business downtime might far exceed that figure. "In the previous world, when you had a disaster, the first thing companies would do was shut their doors [but today] resilience is about how you keep your front door open even when you're under impact, and how quickly you go back to your regular programmes," says Mr Khanna. Losses accumulate in multiple areas: internal response and recovery costs, lost revenue from business interruption, payments to threat actors, and external liabilities such as fines and legal claims (see Figure 2).

Figure 2: Ransom's retreat
Share of total cyber losses by cost category, 2019-24 (%)



Source: Verizon[3]

> **"In framing the issue of spend allocation, the question is at what point does under-investment become the more expensive option? If you look at expected losses — how severe, how long it could take — [then] when expected loss exceeds cost of recovery, that's when it becomes a real issue."**
>
> **- Noémie Heuland**, CFO at Moody's

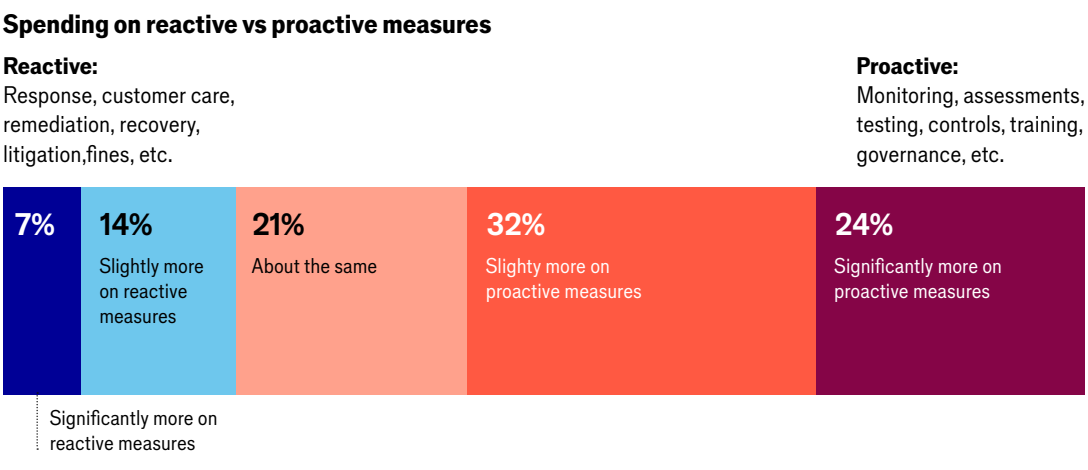
According to Verizon, business interruption now carries the highest financial exposure from cyber incidents, increasing by 51% between 2023 and 2024. Supply chain incidents, a small subset of this, incur the highest costs, with median impacts exceeding US$250,000 and the worst cases surpassing US$100m.[4] Companies are even rethinking years of outsourcing as third-party cyber threats mount. "I've heard a lot of CFOs questioning whether they should bring certain essential functions back in-house," says Noémie Heuland, CFO at Moody's.

Cyber performance is impacting how organisations are valued: investors, insurers, lenders and acquirers now factor cyber risk into their decisions. The consequences of failure can be material: 42% of executives who suffered a cyber incident around the time of a merger and acquisition transaction reported a significant reduction in deal value.[8] Moody's looks at cyber risk as part of its ratings of company debt, given its material impact on credit profiles," notes Ms Heuland.

The tyranny of untested defences

Heightened cyber vulnerability comes at a time when boards are pressuring organisations to accelerate their AI experimentation. According to Gartner, 71% of board members would like to see their organisations take more risks with technology, with AI strategy and speed of adoption at the top of their agenda, but 90% lack a measure of confidence in cybersecurity's value.[9] Just three in ten organisations report well-tested rollback capabilities — the ability to patch and recover from agent-related incidents — our previous research finds.[1]

Figure 3: The misdirected dollar
Proportion of spend allocated to reactive versus proactive measures (%)



Source: PwC[10]

Cybersecurity resilience cannot be achieved by spending alone. Many organisations now face a sprawl from too much technology, which creates complexity, hinders visibility and makes integration harder. "Enterprises are deploying dozens of security tools today, but often don't actually know what to do with them," warns Mr Khanna. "The consoles are disconnected; they don't talk to each other. There is no operating model platform for them." Fragmented tooling weakens defence, but importantly, it slows recovery because no one can see what needs restoring first.

Many organisations remain on the defensive when it comes to cyber strategy. A 2026 PwC survey (see Figure 3) found that 78% of organisations expect their cyber budget to grow this year, yet only 24% are investing significantly more on proactive measures — building and rehearsing recovery and response capabilities before they are needed rather than assembling them under fire. Indeed, the majority are spending the same amount on proactive as on reactive measures.[8] "Resilience is a continuous process. You just can't be resilient for a day," argues Mr Khanna, calling for a shift in success metrics "from mean time to recover to mean time to being resilient."

The upside of getting this right is measurable: Accenture research finds that a 10% increase in security spending towards proactive integrated practices can reduce threat response times by 14%.[11]

The executive equation

Translating resilience into budget decisions requires delicate but essential conversations at the C-level. "The CISO (chief information security officer) wants to cover the [cyber] risk, the risk manager wants to cover risk [across the entire organisation] and the CFO wants to reduce the budget," summarises Rebiah Bardot-Girard, head of cyber risk consulting services at AXA XL. "Because we are talking about three different things, it's really tricky." The CIO has the job of balancing the deployment of a fast-paced AI rollout with the requisite security that comes with it. Each member of the C-suite has to learn the language of their peers in order to support better decision-making.

The cybersecurity function has attracted growing financial resources in recent years, but a June 2026 survey found that 42% of security leaders struggle to demonstrate a clear return on investment (ROI) to boards.[12] To secure continued funding, they will need to shift the ROI narrative from 'activities' to 'outcomes', according to KPMG, which in turn requires better metrics and means of assessing progress. Prevention and resilience are two sides of the same financial equation.

> **"If I look back at the board meetings I was in a few years ago, most of the discussions were focused on the way you budget for insurance safeguards to stop incidents before they happen. The discussion was: how much money do we spend, and where, to prevent a bad thing from happening? The economic lesson of the last three years is that prevention and recovery are different line items with different payoffs. Both matter equally but have different returns, and I think companies in the past had been under-pricing recovery."**
>
> **- Noémie Heuland**, CFO at Moody's

> **"Many entities invest time and energy on the front end, but they don't exercise it, don't test it, don't kick the tires [such as] through business continuity exercises, recovery testing, red teaming, and other rigorous validation efforts that ultimately determine organisational resilience."**
>
> **- Jesus Gonzales**, deputy global practice leader of intangible assets at Aon

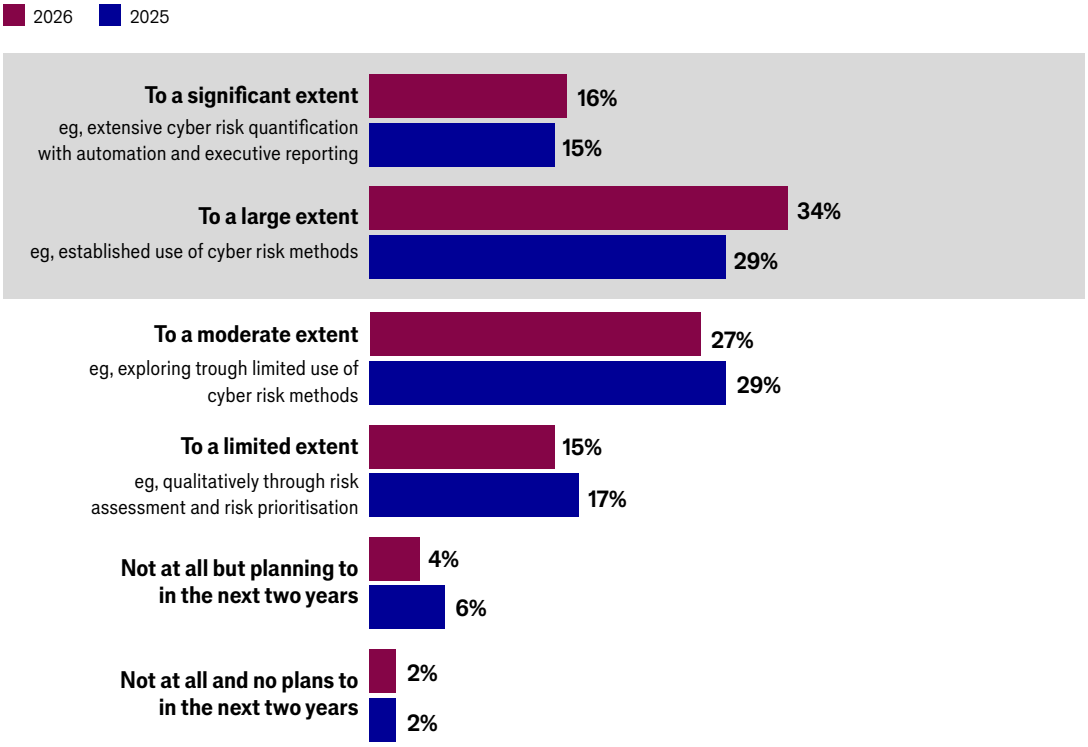
Security controls reduce the likelihood of an incident while resilience determines its impact and cost. Yet companies are only modestly increasing their efforts to measure the potential financial impact of cyber risks (see Figure 4).

While CISOs seek greater investment in cyberdefence, some experts argue that conventional ROI thinking is the wrong framework. "Those who think about ROI for cyber are going down the wrong path," says Al Tarasiuk, the CISO at Citi.

"You can't use financial output as a measure of how good your cyber programme is." Mr Tarasiuk says companies cannot predict the cost of a breach, the regulatory fine, or the reputational damage, especially in sensitive sectors like financial services. "Mature thinking is about risk reduction; you invest what you need to drive down the risk to your business. The board sets the tone of how much risk they want to take, and you build a programme around that."

Figure 4: The phantom metric

Share of executives performing some form of cyber risk financial measurement (%)



Source: PwC[13]

> **"If the CISO is pitching a CFO on stopping zero-day exploits, the budget discussion goes nowhere. But if the CISO can translate that into CFO language — what is the value per dollar, what is the regulatory fine exposure, what does it cost us to be down — and tie it to something like DORA (the Digital Operational Resilience Act), which is non-negotiable, that's how you make the case."**
>
> - **Ashish Khanna**, managing director of global security services at Verizon

Major insurers have even started carving AI-related liabilities out of their policies.[14] From January 2026, the Insurance Services Office excluded AI-caused harm from its standard liability coverage,[15] leaving businesses to absorb more risks themselves. While global premiums for cybersecurity doubled between 2020 and 2025 to more than US$16bn, according to insurance company MunichRe, the vast majority of cyber risk is not insured, representing less than 1% of the total property and casualty insurance premium volume that year.[16]

The conversation needs to shift from whether cyber resilience matters to how organisations assess its value. "Having cyber done properly at the beginning will help you grow your company, not only on the cyber side," argues Ms Bardot-Girard. "It gives you resilience for the company and for the business too." Until CFOs can calculate downtime and associated losses as precisely as they calculate ransoms, budgets will stay misaligned and defences untested.

"You can't bring cyber risk to zero," concludes Mr Tarasiuk at Citi. "There will always be some exposures and you [need to] know what they are." The test for leaders is proving they actually know where those exceptions sit, and how much they cost — the harder work still ahead for the industry as a whole.

References

1. Economist Enterprise, "Power without control: Keeping control in the age of agentic AI", 2026: https://insights.economistenterprise.com/technology-innovation/ctrlz
2. Ocean Tomo, "2025 Intangible Asset Market Value (IAMV) Study", February 2026: https://www2.oceantomo.com/l/710293/2026-02-10/bwjylz/710293/1770735713Uklc7AQh/Ocean_Tomo_2025_IAMV_Study_02_09_26.pdf
3. Verizon, "2026 Breach Impact Study: The Financial Costs of Data Breaches", June 2026: https://www.verizon.com/business/resources/reports/2026-breach-impact-study-dbir.pdf
4. Verizon, "2026 Breach Impact Study: The Financial Costs of Data Breaches", June 2026: https://www.verizon.com/business/resources/reports/2026-breach-impact-study-dbir.pdf
5. S&P Global, "Generative AI experiences rapid adoption, but with mixed outcomes", May 2025: https://www.spglobal.com/market-intelligence/en/news-insights/research/ai-experiences-rapid-adoption-but-with-mixed-outcomes-highlights-from-vote-ai-machine-learning
6. Semafar, "Chinese AI agent attempts unauthorized crypto mining," July 2026, https://www.semafor.com/article/03/09/2026/chinese-ai-agent-attempts-unauthorized-crypto-mining
7. Tech Crunch, "European Parliament Blocks AI on lawmakers devices citing cybersecurity concerns," February 2026: https://techcrunch.com/2026/02/17/european-parliament-blocks-ai-on-lawmakers-devices-citing-security-risks/
8. FTI Consulting, "FTI Consulting study reveals cybersecurity attacks are an increasing threat to M&A", 2026: https://fticonsulting.gcs-web.com/news-releases/news-release-details/fti-consulting-study-reveals-cybersecurity-attacks-are/
9. Gartner, " Gartner survey finds 90% of non-executive directors lack a measure of confidence in cybersecurity value", November 2025: https://www.gartner.com/en/newsroom/press-releases/2025-11-24-gartner-survey-finds-90-percent-of-non-executive-directors-lack-a-measure-of-confidence-in-cybersecurity-value
10. PwC, "New world, new rules: Cybersecurity in an era of uncertainty", October 2025: https://www.pwc.com/jg/en/assets/global-digital-trust-insights/dti-report-2026.pdf
11. Accenture, "State of Cybersecurity Resilience 2025," June 2025: https://www.accenture.com/content/dam/accenture/final/accenture-com/document-3/State-of-Cybersecurity-report.pdf
12. KPMG, "2026 Cybersecurity & Technology Risk Survey", June for2026: https://kpmg.com/us/en/articles/2026/cybersecurity-technology-risk-survey-ciso-resilience.html
13. PwC, "New world, new rules: Cybersecurity in an era of uncertainty", October 2025: https://www.pwc.com/jg/en/assets/global-digital-trust-insights/dti-report-2026.pdf
14. Financial Times, "Insurers retreat from AI cover as risk of multibillion-dollar claims mounts", July 2026: https://www.ft.com/content/51b55431-30e8-4eb3-9730-f5e89c24ad56
15. Fenwick, "The end of 'silent AI'? Emerging AI exclusions, coverage fragmentation, and practical implications for policyholders", June 2026: https://www.fenwick.com/insights/publications/end-silent-ai-emerging-ai-exclusions-coverage-fragmentation-and-practical-implications
16. MunichRe, "From Gaps to Gains: Protection Gap in Cyberinsurance," September 2025: https://www.munichre.com/en/insights/cyber/cyber-protection-gap.html