CORPORATE FINANCE AND STRATEGY

When Cybersecurity Becomes Cyber Strategy

By Vanessa Lyon, Sushmita Banerjee, Sid Sankaran, Liana Shalev, Mike Ford, and Bryan Comis

ARTICLE SEPTEMBER 04, 2025 8 MIN READ

Cyberattacks are no longer technical events. They are business threats. The fallout from an attack can continue for months, with the average breach taking 258 days to contain. And the cost to repair compromised systems can be high, with the median cost for megabreaches now at $52 million.

No one is immune. Since 2019, over a third of S&P 500 companies have reported cyber incidents. The market punishes the unprepared, especially when attackers breach a company's "crown jewels"—the core systems, data, and platforms that drive revenue, customer trust, and operational continuity. Yet despite these rising stakes, and increasing awareness among leadership, many firms

still treat cybersecurity as an IT line item. The conversation may have moved from the server room to the boardroom, but the mindset hasn't caught up.

A risk-based cybersecurity strategy breaks this mold. It redirects cyber investment to what matters most, focusing protection on high-value assets, not just perimeter controls. The data is clear: it's not how much you spend, it's how precisely you protect. Cybersecurity must be reframed as a business discipline that brings together technology, operations, and the executive team to safeguard the organization's most valuable functions and protect shareholder value.

Cyberattacks are escalating—and guaranteed security is a myth.

Many firms still believe that technological sophistication equals failsafe protection. But research tells a different story. Over 60% of companies in highly cyber-mature sectors like technology and finance have reported breaches. (See Exhibit 1 and 2.)

EXHIBIT 1

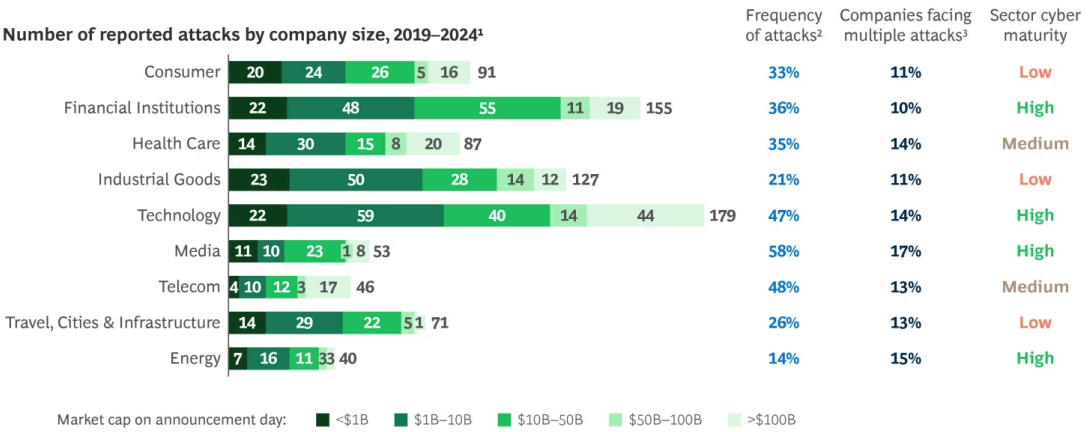
Breaches can wipe out 5% to 10% of market cap overnight; cybersecurity should already be a top priority

Sources: University of Maryland Cyber Events Database (publicly announced attacks 2014–2024 October); S&P Capital IQ; BCG ValueScience Center®; press reports; BCG analysis.
[1]Share price declines 10 days after announcement; marked to relevant index for normalization; includes all US and European attacks on public.
[2]"Crown jewel" assets refer to critical, revenue-generating assets that a company relies upon to effectively deliver goods and services.

EXHIBIT 2

Attack vulnerability is widespread, regardless of cyber maturity

Over the past five years, ~850 cyber attacks on US and European listed companies across a range of industries and size were publicly reported



Sources: University of Maryland Cyber Events Database (2014–2024); S&P Capital IQ; BCG ValueScience Center®; BCG CISO survey (2024); BCG analysis.
¹2024 year to October.
²Percentage of companies on the S&P 500 and S&P 350 Europe that have reported attacks since 2019.
³All US and European listed companies that have announced more than one attack, as percentage of all US and European listed companies that have announced attacks

That's why leadership matters. Executives must plan as if breaches are inevitable; they must understand the risks, prepare for impact, and build the muscle to respond quickly and recover strongly.

Cyber breaches destroy reputation and long-term valuation.

Cyberattacks don't just disrupt systems. They erode customer trust, damage brands, and depress long-term market value. Stock markets respond harshly to cybersecurity lapses. Among impacted companies, nearly one in six (17%) experienced share price declines greater than 5%.[1]

The effects are especially severe when sensitive consumer data or core systems are compromised. One consumer products company suffered ransomware attacks that disabled e-commerce platforms and compromised customer, employee, and supplier data. The result: a 7% decline in market value. And the damage often lingers. Over 60% of companies that experience an initial share price drop following a cyber incident continue to underperform a year later.

But some recover faster and better. When a 2021 breach at a global carmaker compromised more than 3 million customer records, a swift technical resolution and clear, transparent communication helped the company regain market confidence quickly. Clear response plans and strong communications are no longer optional. They are what separate companies that recover from those that don't.

Cybersecurity decisions are business decisions.

For too long, boards have treated cybersecurity as a technical issue that was delegated, siloed, and out of sight. With both the financial and reputational stakes rising, some companies have begun to make the necessary shift. But many still lack a business-wide view, putting their organizations at substantial risk from increasingly sophisticated threats. Cybersecurity today must emphasize business continuity, customer confidence, and operational integrity.

Leading firms are embedding cybersecurity into broader strategic planning and executive performance. A global manufacturer recently integrated cyber metrics into executive dashboards and performance evaluations, making cyber resilience a measurable, accountable business-wide priority. The result: faster decisions, tighter response coordination, and sustained stakeholder trust.

Treat cybersecurity as business insurance.

Cybersecurity, like business insurance, isn't about preventing every loss. It's about reducing the impact when things go wrong.

Breaches are inevitable. What matters is whether the organization can contain the damage and get back to business. That means planning for recovery as seriously as you plan for disruption, because the costs of delay are real: operational paralysis, customer attrition, and valuation loss.

A risk-based approach offers several key advantages.

Cyber spend is often misinterpreted as a proxy for readiness. But data and experience show that there's no direct correlation between budget size and breach resilience. One major retailer suffered a severe breach through a third-party provider, despite heavy investment in cybersecurity and best-in-class tools. The incident emphasizes that spending alone, in the absence of a robust cyber strategy, is not enough to protect against harmful attacks. Where and how you spend your cybersecurity budget is what matters.

A risk-based approach to cybersecurity provides precision over blanket coverage. In this model, recovery isn't an afterthought; it's designed into the strategy. Critical systems are prioritized, crisis roles are rehearsed, and leadership is ready to act on Day One.

Broadly, cybersecurity strategies fall into three categories, from a limited approach to full-scale battle mode:

- *Compliance-driven.* Light, uniform controls spread across all assets. Easy to check the boxes, but often leaves core systems underprotected.
- *Risk-based.* Security tailored to what matters most—concentrated around "crown jewels." Lighter protection is applied elsewhere, freeing up budget and agility.
- *Military-grade.* Heavy protection applied everywhere. Thorough but expensive, inflexible, and often restricts digital progress.

The risk-based approach is the sweet spot—and is gaining momentum for a reason. After suffering a breach, another retailer restructured its entire cybersecurity posture around business-critical functions. By quantifying risk at the asset level and aligning protection accordingly, the company strengthened its resilience without slowing digital growth.

This is what effective cyber strategy looks like: focused protection, not friction. And that precision doesn't just contain risk, it supports value creation. When executives know their crown jewels are protected, they move faster, approve bigger bets, and scale innovation with confidence. From AI integration to digital customer platforms, secure-by-design strategies unlock speed, trust, and sustainable growth. (See Exhibit 3.)

EXHIBIT 3

To protect critical assets efficiently, companies must take a risk-based approach to prioritize high-ROI cybersecurity investments

Sources: BCG analysis and case experience.

Building cyber resilience is a team sport.

Leaders need to have a clear view of their cyber exposure across the organization, understanding both their crown jewels and the third-party risks. They also must have a firm grip on resilience—such as business continuity and crisis management plans—and governance, including executive involvement in cybersecurity decisions and board fluency on cyber topics. Threat assessment methods, such as BCG's proprietary Cyber Exposure Screener, can help leaders calibrate sector-level risks, find critical gaps in the organization, and determine where to prioritize their efforts.

Cyber resilience is about collaboration and partnership. It is no longer the sole responsibility of the information security or IT department. Top-performing companies unite business leaders with technology teams to jointly define risks, prioritize assets, and practice coordinated incident response plans. This partnership helps drive faster recovery, protect critical operations, and preserve trust.

Every function must be able to respond to an incident, even if the breach directly targets another area of the business. To prepare, leading firms conduct scenario testing with full organizational participation. A global insurance group recently trained its leadership team and board through a full-scale cyber simulation involving actors posing as reporters, testing both media response and cross-functional coordination. Building capabilities at the top enabled the entire organization to adopt a strong cyber posture.

These exercises shape a culture of readiness across the company. They foster a shared understanding of what is at stake and who needs to act when breaches occur. In resilient organizations, cyber strategy becomes everyone's responsibility.

Implement a tailored risk-based cybersecurity approach.

Leaders can implement a risk-based approach through the key actions outlined in Exhibit 4.

EXHIBIT 4

Key steps for developing a risk-based cybersecurity strategy

Source: BCG analysis.

Companies that recover well from cyberattacks have one thing in common: engaged leadership. When Maersk was hit by the NotPetya malware in 2017, then CEO Søren Skou did not delegate the crisis response—he led it. He participated in every meeting, directing real-time decisions across port operations and customer communications. Daily updates detailed which systems were online and empowered frontline staff to meet customer needs without budget constraints. That direct leadership involvement was instrumental in maintaining customer trust and operational continuity.

Cybersecurity is no longer a cost center or a compliance line. It's a lever of enterprise value. In today's digital economy, companies that adopt risk-based strategies outperform not because they spend more, but because they protect what matters most. Precision wins. And the companies that know where to focus—on the crown jewels, on resilience, on recovery—aren't just more secure. They are more trusted, more agile, and better positioned to lead in an increasingly digital world. In a world where every digital initiative carries risk, cybersecurity is no longer a gatekeeper; it's the green light for growth.

Authors

Vanessa Lyon

Managing Director & Senior Partner
New York

Sushmita Banerjee

Managing Director & Senior Partner; Corporate Finance & Strategy Regional Practice Area Lead
New York

Sid Sankaran

Partner
New Jersey

Liana Shalev

Partner
Tel Aviv

Mike Ford

Project Leader
New York

Bryan Comis

Managing Director & Partner
New York

ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

1 Measured as relative to the industry index for the company. For example, if a manufacturing company's share price drops 5% and the Industrials index is up 3%, this would be an 8% relative decline. The methodology normalizes impacts across different industries and accounts for systemic market movements.