INVESTOR INSIGHT

Cybersecurity: Governance Matters

Cyber risk is now a ubiquitous concern for most of the companies we evaluate across sectors and geographies. Breaches — when they occur — can be significantly disruptive to operations, costly, and consume considerable management attention.

Executive summary

Cyber risk is now a ubiquitous concern for most of the companies we evaluate across sectors and geographies. Breaches — when they occur — can be significantly disruptive to operations, costly, and consume considerable management attention. They also have the potential to cause serious reputational damage, which can hit consumer confidence and in turn can affect valuations. For investors, these events can become financially material depending on a variety of factors.

Faster vs. slower recovery

Companies that experience a breach in their cyber security emerge from the fallout at different speeds, often based on similar factors.

Faster recovery

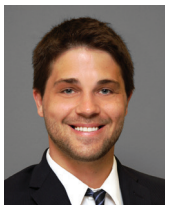
- Transparent and immediate management response
- Strong pre-existing governance and controls
- Limited operational disruptions resulting from the breach

Slower recovery

- Weak governance before the incident
- Delayed disclosure or public response
- High involvement by regulators
- Already-fragile business model

AUTHORS

POOJA DAFTARY
Equity Research Analyst



DAN POPIELARSKI
Strategist,
Client Sustainability & Strategy

Governance is a key differentiator

Because cyber risk is ubiquitous, investors need to understand how companies manage it.

Not all breaches are equally concerning; outcomes diverge meaningfully depending on a few underlying characteristics. At one end of the spectrum are incidents where the operational impact is limited, either because downtime does not materially disrupt customers, the firm's governance and risk structures allowed for quicker identification of the breach, or because the data exposed is not highly sensitive. In these cases, the disruption is time-bound, systems are restored quickly, and knock-on effects are limited. In addition, the financial impact is usually limited to one-off costs, with relatively quick normalization in both operations and the market's sentiment towards the company.

At the other end of the spectrum are incidents where recovery is slower and the consequences extend beyond the initial event. In our experience, governance in these situations is often weaker, or controls are inconsistently applied. This results in the delayed detection of a breach, which in turn causes communication to be reactive rather than proactive. Regulatory scrutiny may also be higher due to what are later identified as obvious shortfalls in risk management, prolonging the overhang. In the most extreme cases, pre-existing fragility in the business model may severely upend the company. In these instances, the impact of the initial breach compounds, as direct costs are only part of the story — operational disruptions last longer, customers are more significantly impacted, and management attention is diverted from day-to-day strategy execution. The market tends to treat these as structural challenges rather than temporary issues, creating a meaningful valuation overhang.

We feel most companies sit somewhere along this spectrum, but differences in preparedness and response explain why some cyber events are short-term earnings issues while others become multi-year valuation concerns.

Cyber risk and the emergence of AI

The emergence of artificial intelligence is making cybersecurity an even more important risk for companies to manage because it increases both the size and complexity of their potential digital vulnerabilities. AI models use large amounts of sensitive data and are connected to many systems and third parties. This creates more entry points for cyberattacks than have existed to date. At the same time, cyber criminals are also using AI to improve their methods. They can now automate phishing, fraud, and the search for system weaknesses, making attacks faster and more advanced.

AI itself can also create cybersecurity risks: a whistleblower found that Anthropic's Fable 5 could be jailbroken in a way that had the potential, given its advanced capabilities, to cause significant cyber risk for a substantial number of companies and individuals around the world. The model was able to identify thousands of critical, previously unknown software vulnerabilities on its own. This led to the model being banned until July 1, when it was shown that other, less capable models could be similarly manipulated, meaning this vulnerability was not unique to Fable — and making the risk even more widespread.

This increases the potential impact of cyber incidents, especially as AI becomes more integrated into core business operations. From a governance and investment perspective, cybersecurity is now an important sign of how well a company manages risk. Companies need stronger oversight, better data protection, and clear incident response plans. Moreover, oversight should not just be the responsibility of management; companies truly managing cyber risk have board oversight, as well. They also need to manage new risks, such as AI model manipulation and data leaks. Now more than ever, cybersecurity is a key part of enterprise risk management and the responsible use of AI.

Cyber risk assessment framework

We have developed the following framework to guide our assessment of the financial materiality of cyber events and the read-through to corporate culture, operational risk, and valuations. This framework is grounded in four pillars:

1 GOVERNANCE & ACCOUNTABILITY

Clear oversight of cybersecurity needs to be present at a management and board level, which requires individuals with proper experience and training in this area. This influences how quickly issues are identified, escalated, and addressed. Where this pillar is weak, detection is slower, response is less coordinated, and outcomes tend to be worse.

2 THIRD-PARTY EXPOSURE

Cyber risk often impacts a company through third-party software or the use of systems by contractors and non-employees. Some companies operating across complex ecosystems or with heavy outsourcing tend to have more points of vulnerability, making oversight of these relationships critical.

3 PRIVACY

Companies keep substantial amounts of customer information, but they need clear rules regarding how much data is retained, who has access to it, and how it is stored. Though there are regulations on data privacy for companies across various jurisdictions, their level of strictness may vary.

4 INCIDENT READINESS & RECOVERY

A company should understand, and plan for, how a cyber incident could impact different business units or product/service lines to ensure the proper risk controls are in place. Companies must also simulate breaches and responses, as well as the likely steps needed to recover systems, operations, and investor or customer trust in the event of a breach. This is also where basic control failures can extend downtime in ways that become financially meaningful.

This framework maps directly to broader operational discipline and risk management concepts that are integrated in our fundamental investment analysis. Cyber risk awareness provides an additional, real-time test of the effectiveness of the risk management systems that we assess.

Case study: Coupang

Coupang is an example where the specific cyber security incident quickly became secondary to more general governance and transparency concerns. Coupang is an e-commerce company that operates out of South Korea, often referred to as South Korea's Amazon. The company disclosed a large-scale customer data breach affecting tens of millions of users, but the timing and sequencing of those disclosures raised questions around information asymmetry and whether bad news was being "managed" rather than communicated transparently. Following the incident, the stock sold off meaningfully and underperformed benchmarks. More importantly, the situation highlighted existing governance concerns. Founder control was concentrated through a dual-class structure, which limited board independence. In that structure, escalation and challenge became more difficult, particularly during a stress event.

From an investment perspective, the issue was not just the direct cost of the breach, but a change in our view on the quality of and confidence in management's decision-making. We determined that the company's decision-making was not sufficiently balanced, and that trade-offs between legal positioning, operational response, and stakeholder communication were poorly managed. When disclosures of this nature are delayed or incomplete, confidence in management tends to weaken. In this context, the cyber incident became a lens into governance quality where the risk was less a one-off hit to earnings and more a sustained discount applied to the business.

Case study: LY Corporation

LY Corporation is a Japanese internet and technology company that operates a messaging app, e-commerce, and digital advertising as well as managing fintech and mobile payment solutions. LY was a useful contrast to Coupang because their issues were less about disclosure and more about operational complexity and execution. The Askul ransomware incident exposed basic control failures at a subsidiary level, which in general is not unusual. The more important question was what the company's response to the attack said about the overall business structure. In LY's case, execution was relatively decentralized across a portfolio of businesses, with systems built on legacy infrastructure and multiple integrations. This increased both the likelihood of incidents and the operational impact when they occurred. Communication and escalation across subsidiaries could be slower and recovery could take longer because systems were not fully standardized. There was also a regulatory issue, particularly around LINE (a messaging app run by LY), which increased scrutiny and extended the tail of these events.

At the same time, there were clear signs of improvement. Controls were being strengthened, frameworks were becoming more consistent across subsidiaries, and management showed willingness to address issues and invest in systems. From an investment standpoint, this created a different risk profile. While the company has taken clear steps to improve their cyber risk governance, the current organizational structure indicates that cyber risks will likely persist: LY still has a number of subsidiaries from different industries, with different risk structures and separate management teams. Governance credibility is less of a concern, but operational volatility is likely to remain. Incidents may continue to disrupt execution and consume management time and effort, which can distract from the operational execution we want to see. These and more questions and considerations went into valuing the company, but the key question is whether improvements are happening quickly enough to reduce the frequency and severity of those disruptions. Our view is that the risk–reward profile is still positive given the company's upward trajectory of change in governance combined with an undemanding valuation.

Broader case studies and read-throughs

We see similar dynamics across other sectors. Below are a few examples of past breaches and how they affected the companies:

Health care

In health care, the Change Healthcare incident highlights how financially material cyber events can become when they hit critical infrastructure, with both direct costs and broader operational disruptions.

Retail

In retail, Marks & Spencer illustrates how timing amplifies impact, as a ransomware attack disrupted its supply chain during a critical holiday shopping season. Interruptions during peak periods can have outsized financial consequences even if the underlying business remains intact.

Telecom

In telecom, SK Telecom shows how regulatory and legal overhang can persist well beyond an initial incident, as there was a financial penalty of $200 per user from regulators.

Across these examples, the interaction between cyber events and the underlying business model is key. Ultimately, cyber risk reinforces a broader investment principle: specific events matter less than what they reveal. Because breaches are now more widespread than ever, their occurrence alone provides limited insight; the real signal lies in how effectively companies anticipate, absorb, and recover from disruption. This makes cybersecurity a valuable lens through which to assess governance quality, operational resilience, and management credibility under pressure. Rather than attempting to isolate cyber as a standalone valuation input, we incorporate it into our broader assessment of execution risk, using incidents as evidence of how companies behave under stress and how much uncertainty we are underwriting. In this way, cyber serves not just as a risk factor, but as a continuous, real-time test of the durability of the investment case.