NOMURA
Connecting Markets East & West

Why Cybersecurity is the Biggest Hidden ESG Risk

- **Cybersecurity is emerging as a major ESG factor for investors, with strong alignment to financial and investment risk, growing regulatory scrutiny, and real-world impact**
- **Corporate cyber-attacks are growing in severity and frequency with global loss estimates from cybercrime reaching $6 trillion in 2021**
- **We integrate Cybersecurity directly into our Credit ESG Scoring model as a "Governance" factor for corporate debt investment strategies as it reflects a company's overall governance structure**

Cybersecurity is fast becoming the top global risk by impact and likelihood along with climate change and geopolitical conflict. In response, investors need an efficient model to integrate cybersecurity into their investment decisions.

ESG integration is the consideration of market material, non-financial factors in investment analysis to improve risk-adjusted-returns in a way that also addresses important socioeconomic and environmental challenges. Carbon emissions and climate change are prime examples of how shifts in awareness and market pricing of ESG risks can lead to real-world impact. For example, it is now mainstream practice for investors to integrate greenhouse gas (GHG) emissions disclosures into the investment processes.

As a result, trillions of dollars of capital are currently being allocated and priced according to investor perceptions of corporate carbon performance. Due to this repricing of corporate risk and valuations, firms have a powerful incentive for emission reductions in support of global climate mitigation efforts. Investors thus achieve real world impact and avoid investment risks by addressing the "market failure" of such previously unpriced negative externalities. By implication, investors are incentivized to identify new non-financial ESG factors with the potential to materially affect market pricing.

Cybersecurity is emerging as a major next generation ESG consideration for investors, with strong alignment to financial and investment risk, growing regulatory scrutiny, and the potential for real-world impact.

Financial Materiality of Corporate Cybersecurity Risk

Investors have a growing interest in assessing the underlying cybersecurity risk inherent in their corporate investment portfolios. Cybercrime affects individual enterprises through increased frequency of data breaches and ransomware attacks, higher corporate cyber defense and insurance spending, and reputational damage. Large-scale cyberattacks can cause operational and business disruption, and generate significant litigation risk.

Cybercrime rates are growing in severity and frequency as economic digitalization expands the cyber "attack surface" available for hackers to exploit. Estimates of the rate of cyber-attacks per company are 31% higher in 2021 compared to 2020 with the average cost for individual data breaches in 2022 reaching $4.35 million. Ransomware has become a major concern for businesses, with survey data showing that 83% of organizations experienced a ransomware attack over the past two years. The most commonly demanded ransom amount for US companies is now in the range of $5 to 10 million.

Corporate cyber defense spending is emerging as a major cost for businesses. The overall market for business spending on cybersecurity products and services is estimated to reach $1.75 trillion for the 5-year period from 2021-2025, compared to $1.0 trillion spent from 2017 to 2021. Certain financial firms in the US reportedly spend over $1 billion per year just on securing and protecting digital infrastructure and client data.

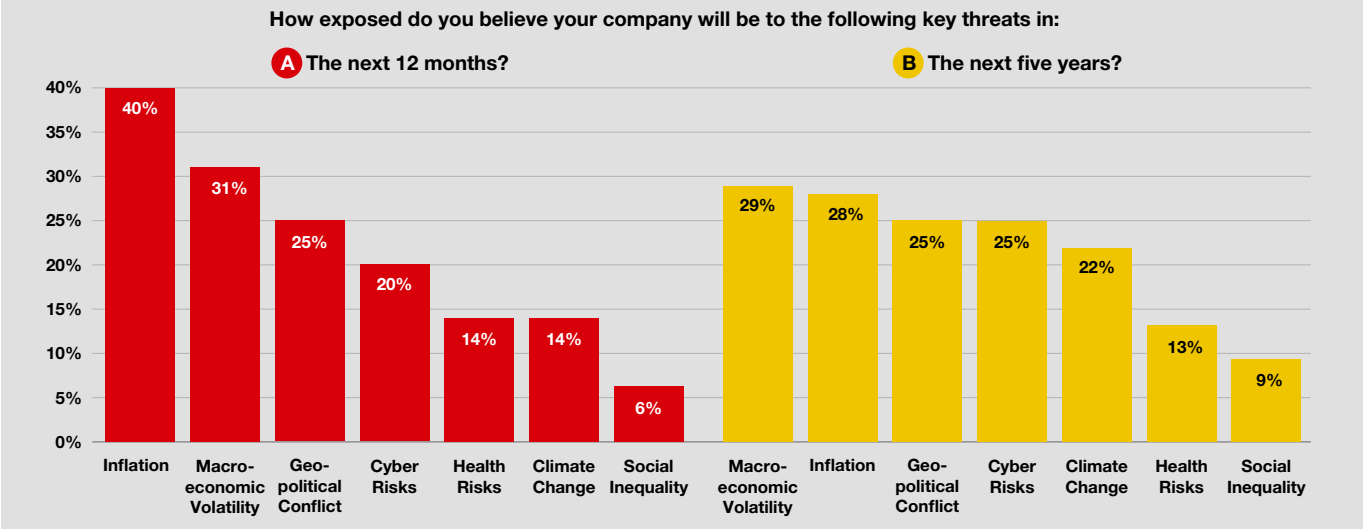
More firms are opting for cyber-insurance, with one US study finding that insurance uptake rates rose from 26% in 2016 to 47% in 2020. The overall cyber insurance market is predicted to grow to $34 billion by 2031, from approximately $8.5 billion in 2021.

Recent major cyberattacks have targeted hospitals and pharmaceutical companies, travel and leisure companies, financial services and energy infrastructure operators. Individual events not only disrupt operations and result in hundreds of millions of dollars in business impairment and legal liabilities, they can also compromise sensitive personal data and may threaten national critical functions. In one high profile case in 2017, Chinese military hackers exploited an unpatched software vulnerability to infiltrate a consumer credit reporting agency in the United States. The cyber-attackers stole personally identifiable information including names, addresses, and Social Security Numbers linked to detailed financial records of approximately 145 million people. When the company disclosed the data breach, its stock declined by as much as 35% and credit spreads on its Investment Grade-rated debt widened by 118 basis points.In 2019, the company reached a settlement with US regulators for at least $575 million in fines, penalties, and consumer restitution.

In 2019, the company reached a settlement with US regulators for at least $575 million in fines, penalties, and consumer restitution.

From a broader societal perspective, inadequate protections in cyberspace can lead to macro-economic damages with national strategic implications, industrial espionage, the erosion of incentives for innovation and investment, and the violation of data privacy. They also include threats to the critical functions that underpin economic and national security, public health, and the safety and freedom of citizens. Investors are increasingly aware that the risks from Cybersecurity are not limited to the companies directly affected but also extend to the entire society that underpins the economy and market valuations.

Figure 1: Cyber Risk is among the Biggest Threats over the next 5 years



Source: PwC's 26th Annual Global CEO Survey.

Economic damages from cybercrime and cyber-espionage are growing at an immense scale. Some sources estimate that global annual losses from cybercrime may reach $10.5 trillion *per year* by 2025 from $6 trillion in 2021. In comparison, a 2021 reinsurance company report estimated economic losses from climate change at $23 trillion *cumulatively* by 2050. While differences in methodology and statistical sampling make it difficult to compare these figures directly, the implication is that the economic impact of cybersecurity may be at a similar scale as climate change. Reflecting this, Cybersecurity consistently ranks in the top 5 global risks in perception surveys of global CEOs and decision-makers together with climate change and geopolitical conflict.

Market participants are increasingly aware of the growing direct and indirect costs from weak corporate cybersecurity. Based on this trend, more investors are now beginning to incorporate cybersecurity performance as a non-financial (ESG) factor for analysis in corporate investment.

Nomura's Approach to Cybersecurity in Credit Analysis

We have developed a proprietary approach to systematically and quantitatively integrate cybersecurity into credit analysis.

1. Cybersecurity risk as a "Market Failure"

As part of our approach, we considered the current challenges faced by the market for recognizing, assessing, and pricing corporate cybersecurity risks.

First, corporate cybersecurity has traditionally been treated as an extension of the IT department, which has led many corporates to view cybersecurity resiliency as a compliance cost to be minimized.

As a result, spending on preparedness is often insufficient relative to the level of risk. Corporate cybersecurity reporting lines and responsibilities are often unclear, and board oversight and expertise in this topic is limited.

Second, cybersecurity has generally existed outside the purview of legislation and regulation. Most digital infrastructure is privately owned, so cybersecurity policies are typically based on "best practice" rather than regulatory requirements. Most cyber incidents and breaches are not publically reported or acknowledged, making it difficult for investors to assess cybersecurity risks.

Going forward, the systematic integration of cybersecurity risks in investment analysis will create demand for more material cybersecurity-related disclosures. At the same time updates to regulation will require more disclosure of breach and mandate greater cybersecurity preparedness.

Third, it is not easy to standardize the evaluation of cybersecurity performance across companies. Cybercriminals opportunistically target areas of weakness with a variety of intrusion strategies, so risk vectors and attack methods are constantly changing. This means that cybersecurity defenders cannot just focus on a specific set of high-risk systems or processes, or rely on any single method of prevention. By extension, investors cannot use a generalized framework for assessing the idiosyncratic cybersecurity risks between companies based on comparative evaluations of known weak points.

Firms do not usually disclose meaningful details about their cybersecurity policies and performance to public investors, and there are legitimate concerns that too much disclosure of cyber vulnerabilities would only attract more cyber-attacks. Together this implies that investors evaluating cybersecurity across companies will have to rely on forecasted measures of cybersecurity preparedness and adherence to best practices as a proxy for cybersecurity risk.

These challenges have made it difficult for investors to comprehensively integrate cybersecurity risks in the investment process. In particular, the lack of comparable cybersecurity performance data has prevented markets from efficiently pricing corporate cybersecurity risks.

2. Adopting Cybersecurity data as a next generation ESG factor

To address the challenge of integrating cybersecurity risk in corporate debt investments, we focus on measuring "cybersecurity hygiene," which is the regular application of best practice that an organization takes to keep its network and data secure, such as patching of known vulnerabilities, strong password requirements, and data backups.

The data required for comprehensively evaluating cybersecurity hygiene as a proxy for cyber risk is becoming more widely available to investors. Traditional ESG data providers tend to provide subjective assessments of issuers' data privacy and protection policies. But such survey methods cannot give an accurate or objective overall measure of organizational cybersecurity performance. A variety of specialized data providers now provide "cyber risk ratings" based on automated measurements of cyber hygiene.

Just as credit risk ratings reflect the issuer's predicted ability to pay back debt with an implicit forecast of the likelihood of default, cyber risk ratings are designed to reflect the organization's overall cybersecurity performance and implied risk of cyber breach or ransomware attack. In fact, some traditional credit ratings firms now integrate cybersecurity risk ratings directly into their corporate credit ratings as a form of nonfinancial (ESG) data. This makes sense as cybersecurity risks can have a direct impact on credit quality and investment returns.

3. Nomura's approach to integrating Cybersecurity data in Credit ESG analysis

We integrate Cybersecurity directly into our proprietary Credit ESG Scoring model as a "Governance" factor for corporate debt investment strategies. This reflects our view that cybersecurity performance reflects an organization's overall governance structure. Good cybersecurity hygiene indicates good corporate governance, and a more attractive corporate debt investment from the perspective of risk-reduction and high quality management.

The 'NAM Credit ESG Score' model outputs are integrated into screening, security selection, risk monitoring, and issuer engagement across all global corporate credit strategies, ensuring that cybersecurity risk signals are systemically reflected in our fixed income investment process.

In addition to the cybersecurity performance of individual issuers, sector-specific cybersecurity materiality is a crucial element for integrating third party cyber risk data into the credit ESG model and for prioritizing engagement with companies. To generate our matrix of material sectors, we analyse the relative risk for each industry sector along three dimensions:

1. **The potential for socio-economic impact and damage from cyber-attacks on the sector**
   The more critical the potential damage to the provision of essential goods and services, the higher the cyber materiality
2. **The observed frequency of cyberattacks against the sector**
   The higher the frequency of cyberattacks against the sector, the higher the cyber materiality
3. **The existing level of cybersecurity sophistication and resource availability in the sector**
   The higher the observed average cybersecurity hygiene for issuers in the sector, the lower the cyber materiality

Based on this framework, we assign the highest cyber materiality to sectors that are the most vulnerable and most frequently targeted by cyber attackers, and where the damage from cyber-attacks on the provision of essential services is potentially the greatest. Cyber hygiene performance data can then be adjusted on a risk-informed basis as an input for the overall credit ESG scoring model.

Finally, the resulting "heat map" of sector-specific cybersecurity materiality acts as a guide for our research and engagement with investee companies.

Conclusion

With growing financial materiality and a rapidly changing regulatory and disclosure environment, corporate cybersecurity is a next generation factor for mainstream ESG investors to integrate into investment decision making. Addressing the "market failure" of insufficient attention to corporate cybersecurity by incorporating it into ESG analysis can incentivize higher performance standards across the board, potentially contributing to better risk-adjusted-returns and socio-economic resiliency as a real world positive impact.

Jason Mortimer
Head of Sustainable Investment – Fixed Income,
Nomura Asset Management

DISCLAIMER