LOMBARD ODIER
INVESTMENT MANAGERS

Investment viewpoint

Cybersecurity: a neglected risk in a digitalised world

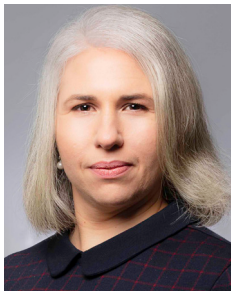
For professional investor use only • Equities

July 2022

Key points

- As the world continues to transform digitally, the threats and risks around cybersecurity continue to follow right behind. However, little work has been done to manage these risks within investment portfolios.
- A lack of data and material framework are some of the reasons why we believe asset managers have not integrated cybersecurity risks into their strategies.
- The healthcare, financial and pharmaceutical industries are those most often targeted. The costs of insurance, training internal teams about risks, and other security measures are far less than the amount that could be lost from a successful hacking attack.
- Investors need to mitigate these risks, which is why we have developed a multilayered approach involving the integration of cybersecurity screening methodologies that we tailor to the needs of an asset manager.

Jeroen van Oerle, CFA
Portfolio Manager
Global FinTech



Rebeca Coriat
Head of Stewardship

Introduction: the need to mitigate risk

Technology and digitalisation have shaped the world, and both continue to evolve at a rapid pace. As the world continues to move through this transformative digital journey, investors must keep up with the trends and risks that can follow.

When thinking about the number one risk in a digitalised world, cybersecurity is top of mind for everyone, yet little has been done to integrate this into the investment process. There is a side to this risk that offers investment returns, namely in the form of cybersecurity software companies and insurance providers. There are several funds, both active and passive, around this theme. There is, however, another side to the issue within portfolio management.

Cybersecurity risks are not concentrated in specific companies or industries. They are omnipresent, as the numbers in this report show. This implies that cybersecurity risks are material and should be considered in the risk assessments in portfolio management. So far, we are unaware of any asset manager integrating these risks beyond the standard subjective inputs from questionnaires by ESG data providers. This is because although everyone is aware of the risks, only a few can translate the technical evidence-based input from cyber tools into portfolio management signals and conclusions. However, at LOIM, we have been researching this topic for the last couple of years and have tested many data sets.

The main issues we found were the following: unstable data, deep technical data, lack of materiality framework and no follow-up with the company. After many trials and errors, we have set up a methodology that tackles all of these points. It is not a perfect prediction tool in mapping out which companies will be attacked. What it does, instead, is assess the company's resilience – whether it can recover quickly from an attack and return to business as usual.

Besides the business continuity angle, there is also more discussion about rules and regulations around cybersecurity. This implies that companies that lag behind in terms of tech stack (a list of all the technology services used to build and run a single application) will likely need more investments than those with strong systems in place. We believe this will influence margins and potentially growth.

Threats are omnipresent

Before diving into the methodology of our risk screening, we must first discuss the cybersecurity market dynamics and map out the threat landscape. The total costs of cybercrime were estimated to be USD 6 trillion in 2021, growing to USD 10.5 trillion in 2025. This implies that if cybercrime were an economy, it would be the third largest after the US and China.[1] On average, there are 2,244 attacks per day.[2] As seen in Figure 1, the average total cost of a single data breach has been increasing steadily during the past couple of years. The pandemic played a role – with more people working remotely in less secure environments, this created more opportunities for cyberattacks.

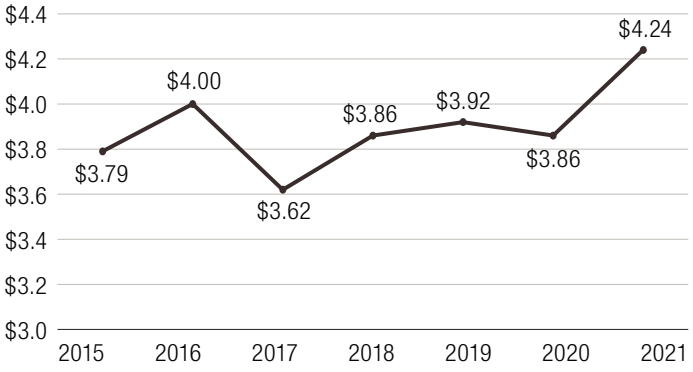
Clear evidence of that can be seen from a breach in April 2020, where half a million Zoom[3] user accounts were compromised and sold on the dark web, enabling criminals to spy on company meetings and act on behalf of representatives of the company, asking others for critical information via chats and other channels. Besides the increase in opportunity for cyberattacks, the number of cyber criminals also increased because individuals had more time to hang around in chat groups and develop hacking skills. The FBI has reported a 300% increase in reported cybercrimes since the pandemic began.[4]

Who is the main target?

The USD 4.24 million shown in Figure 1 is an average cost per breach. Larger companies were targeted more often, and the average total cost of a data breach was positively correlated to size. There is also a correlation between the costs of a data breach and geographic location. The USD 4.24 million is representative for an average European company, whereas the costs in the US and Canada were higher, at USD 9.05 million and USD 5.40 million, respectively. Costs for Latin American and Asian companies were about half the global average. The main reason for these differences is the post-breach response costs. The lost business costs are much higher in the US than in many Asian countries merely because of the absolute size of businesses in the US. In total, 65% of the data breach costs relate to solving the issue and covering business continuity costs. The actual detection and escalation of the breach represents 30% of costs. This makes it clear that the direct costs to minimise the likelihood of an attack and to resolve the issues as soon as possible are much smaller than the after-effects.

Investing in cybersecurity software, a chief information security officer (CISO) and the proper resources for cybersecurity teams pays off. In addition, internal staff training and ensuring a broad presence of cybersecurity awareness and skills across the operation is instrumental in mitigating risk.

FIG 1. GLOBAL AVERAGE TOTAL COST OF A DATA BREACH (USD MILLIONS)



Source: Ponemon, IBM 2021.

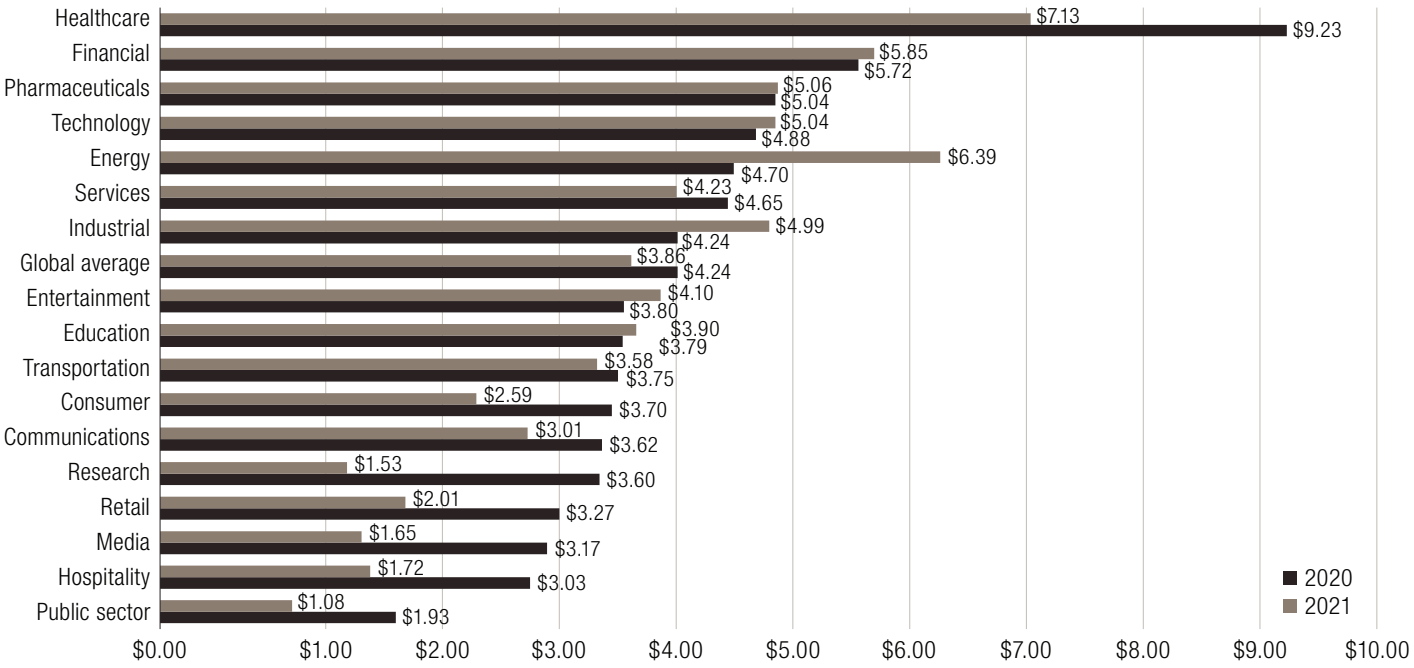
Besides size and country, industry is also an important factor in analysing cybersecurity threats. As seen in Figure 2, the healthcare sector and financials rank highest in terms of the average total cost of a data breach. Put simply: the damage to these industries is much larger than in the public sector or in hospitality, which rank lowest in the list. Given the sensitive nature of financial and health data, these breaches have larger consequences.

Increasing transparency

In December, the EU Parliament approved the Network and Information Security Directive, which will introduce baseline cyber-related risk management resources, reporting obligations, and remedies and sanctions for enforcement for a wide scope of companies. In March, the SEC proposed amendments to rules to enhance and standardise US public companies' disclosures on cybersecurity risk management, strategy governance and incident reporting. The amendments would require companies to periodically

[1] "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," By: Morgan, S. Published on 13 Nov 2020.
[2] Varonis.com, 2021.
[3] Any reference to a specific company or security does not constitute a recommendation to buy, sell, hold or directly invest in the company or securities. It should not be assumed that the recommendations made in the future will be profitable or will equal the performance of the securities discussed in this document.
[4] COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes - IMC Grupo.

FIG 2. AVERAGE TOTAL COST OF A DATA BREACH BY INDUSTRY (USD MILLIONS)



Source: IBM, 2021.

disclose policies and procedures for managing cyber-related threats, and the board of directors' degree of oversight of cybersecurity risks, and to provide updates about previously reported incidents.[5]

The top four industries in Figure 2 have been stable over the past couple of years. This implies that checking cybersecurity risks is crucial for investors exposed to healthcare, financials, pharmaceuticals and technology.

The root of the problem

After establishing which countries, sizes and sectors are breached most, it is important to look at the nature of cyberattacks. There are many ways for hackers to enter company databases, as seen in Figure 3. Some are via software exploits, due to outdated or non-patched software stacks. Others are related to theft of personal details to exploit accounts and enter as a "legitimate" user to extract data and install spy or malware. However, it is difficult to monitor the latter category. It is important to note that many people do not know they are contributing to cyber-intelligence for criminals. They simply fill out their details or do not prevent others from creating tracking profiles, which can be exploited at any stage. In an advanced cybersecurity screening, it is possible to monitor the dark web for intelligence that could be traced back to certain companies via the stolen employee data. This data may not necessarily be used to penetrate the company, but can be used in different attacks related to the employee. Therefore, it is difficult to draw strong conclusions based on that data from an investment perspective. However, CISOs can use these cybersecurity tools to track employees and monitor activities from which critical data has been sold on the dark web.

The first category, attacks via vulnerabilities of software, is easier to measure and can be directly related to the company itself. This is what our cybersecurity rating focuses on. Known vulnerability screening can be seen as a basic hygiene screening. If the company has old software and has not done anything to patch or upgrade known vulnerabilities, it sets itself up as an easy target. This data can be related directly to specific companies and is helpful from an investment perspective.

This information can be used in the fundamental analysis of companies, and also to engage with those that score poorly on cyber hygiene. Investors can ask questions on this topic and present evidence-based findings to management teams or CISOs, which can change the landscape in our opinion, as it puts cybersecurity at the forefront of management's attention.

Lessons from ESG reporting

We have seen similar effects (albeit after many years) with ESG reporting. This refers to the disclosure of data covering the company's operations in the areas of environment, social and corporate governance while also providing a snapshot of the business impact in these areas. It helps investors make better-informed decisions and helps companies implement sustainable business models.

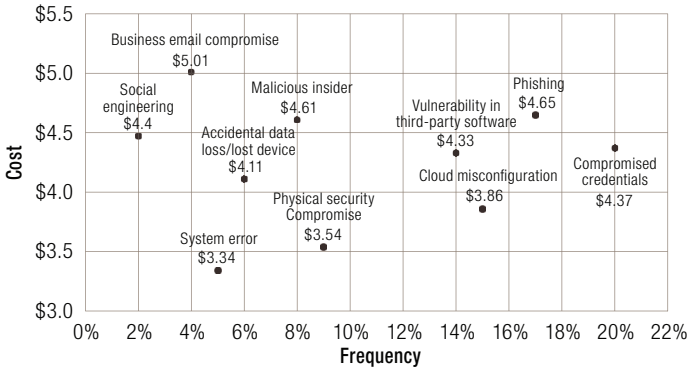
The growth of ESG reporting standards has been triggered by civil society, investors, and regulators all interacting at different moments and demanding openness and reporting on ever-expanding ESG metrics. Indeed, ESG reporting took off in the early 2000s as seen through the UN Global Compact, Global Reporting initiative,

[5] NIS Directive — ENISA (europa.eu); Proposed rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

national corporate governance codes, FSB Task Force on Climate-related Financial Disclosures, EU Taxonomy and more recently, the Taskforce on Nature-related Financial Disclosures framework. The variety and almost exponential increase in reporting standards have focused on environmental, governance and social metrics, and the financial impact of some of the issues. However, very few reporting standards have focused on cybersecurity.

We believe the rise in ESG reporting standards and demands has driven an improvement in these concepts and a deepening in the quality of strongly applied ESG measures. We believe that the rise in cybersecurity reporting should have a similar effect. The arguments above show up in data as well, which is evident from the cost difference between compliance level failures. The average costs in the case of high compliance failures (no processes to detect breaches and mitigate cyber risks) is twice the level of costs related to companies with low compliance failure.[6]

FIG 3. AVERAGE TOTAL COSTS OF AND FREQUENCY OF DATA BREACHES BY INITIAL ATTACK VECTOR (USD MILLIONS)

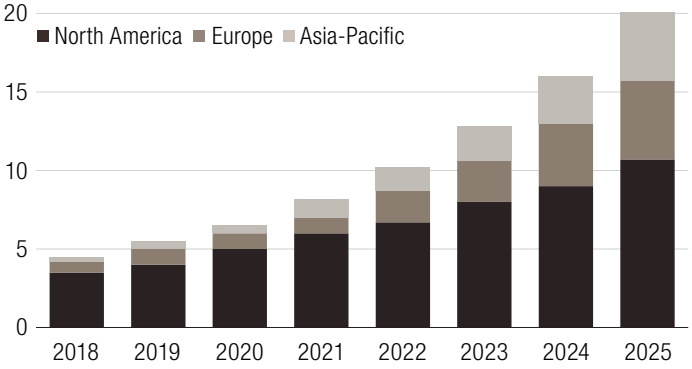


Source: IBM, 2021.

Seeking protection

With these cybersecurity risks and increasing costs of breaches, it makes business sense for companies to try to insure themselves. Figure 4 shows the growth trajectory for cybersecurity insurance premiums. The US is the largest market. That makes sense given the discussion above, where we stated the average costs of data breaches in the US is twice the global average. European adoption is mostly driven by regulation. Cybersecurity insurance is expected to be a USD 20 billion market by 2025. Compared with the estimated USD 10.5 trillion global costs of cyber-attacks, the difference in amount speaks for itself. The cyber insurance market has been key for our rating system. Pure technical cyber data is too far off from financial decision making. Insurance underwriting, however, is much closer to risk management capabilities in the asset management industry.

FIG 4. CYBER INSURANCE PREMIUMS MARKET FORECAST (USD BILLIONS)



Source: Cyber resilience - Annual Report 2020-2021 (insuranceeurope.eu).

The first approach to cybersecurity trends: build a portfolio of cybersecurity companies

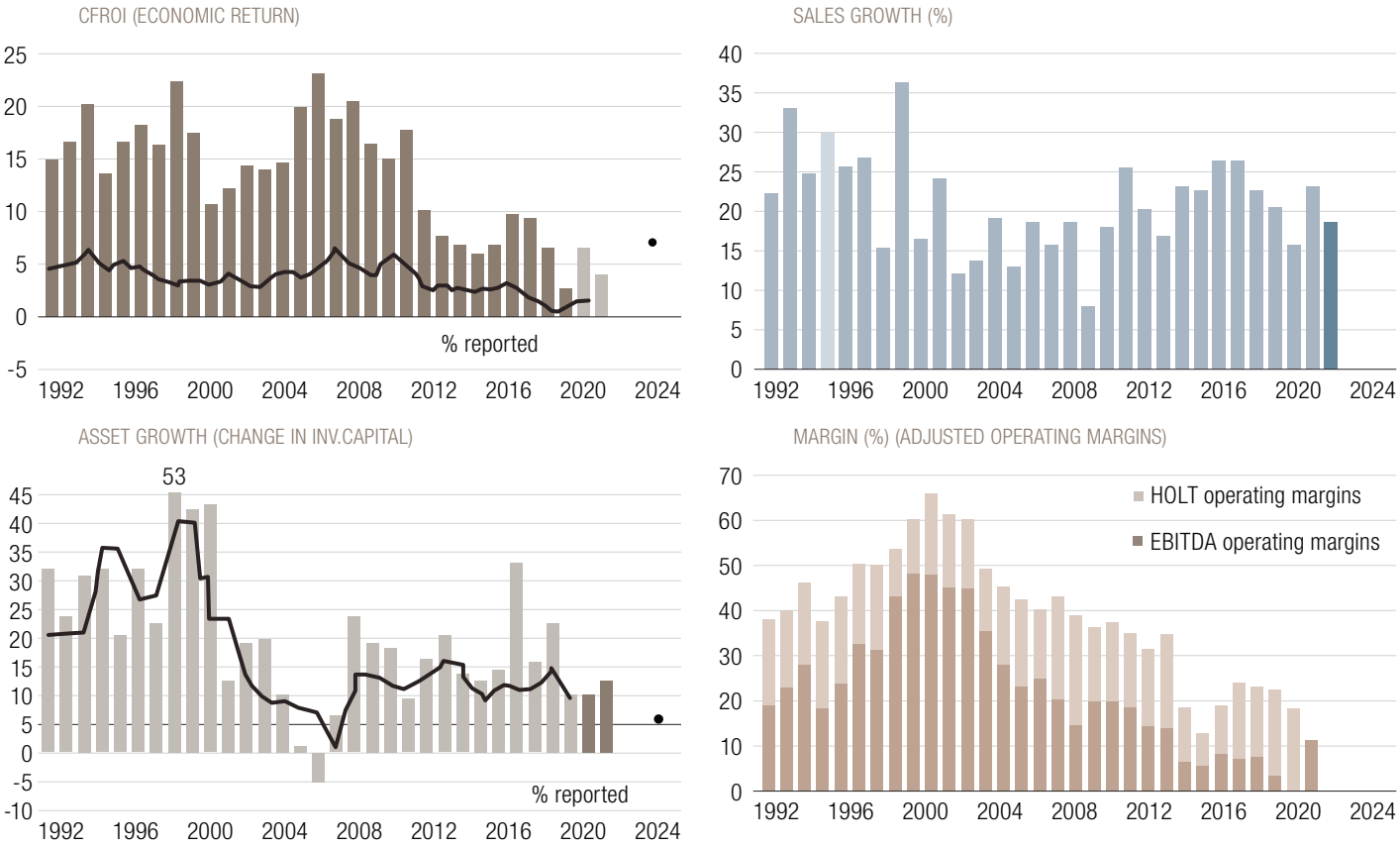
As discussed at the start of this paper, there are two ways to transform information on cybersecurity threats into opportunities in asset management. The first approach is most common. This involves building a portfolio of cybersecurity companies offering software that can be used to defend against and mitigate risks.

This trend-based approach can be applied in either a passive or active portfolio management style. At first sight this makes sense; however, looking beyond the trend to more fundamental research reveals that most cybersecurity firms find it very difficult to generate profit. As seen in Figure 5, the median profitability of all cybersecurity firms added globally has been deteriorating since 2012 and margins have been falling for the last 20 years. During this time, sales growth has been stable. The main reason is that the investments required to keep up with the ever-evolving threat landscape are costly and prevent scale advantages due to custom work.

Another difficulty is defending against the ever-changing attack patterns, which make it challenging for defence software to single out one specific threat. This implies that companies need multiple vendors and solutions for a wide suite of potential threats. These dynamics make it difficult to invest in high-quality companies within this segment. It is not impossible, because there are several strong companies to be found within the cybersecurity space, but the median company typically does not generate strong returns.

[6] IBM, 2021.

FIG 5. MEDIAN CFROI, SALES/ASSET GROWTH AND MARGINS CFROI (ECONOMIC RETURN)



Source: Credit Suisse HOLT custom screen, 2022.

The need for enhanced security

When looking at the cybersecurity threat-prevention landscape, companies need to be secure, vigilant and resilient.[7] Being secure refers to preventive aspects. This entails elements such as authentication, DDOS protection, virus scanners and endpoint protection. It also refers to soft factors such as cybersecurity training, education and awareness. Vigilance refers to the efficient and effective discovery of emerging threats and the required response to incidents. This is where advanced cybersecurity solutions such as database protection, behavior-monitoring and data analytics play a vital role. The final element, resilience, refers to the response aspect of a breach involving cyber wargaming, managed security service providers and insurance solutions.

SECURE	VIGILANT	RESILIENT
Preventive aspects	Discovery of emerging threats and appropriate response	Rapidly adapt and respond to cyber disruptions
• Infrastructure protection • Vulnerability management • Application protection • Identity and access management • Information privacy and protection	• Advanced threat readiness and preparation • Cyber risks analytics • Security operations center • Threat intelligence and analysis	• Cyber incident response • Cyber wargaming • Cyber risk insurance

Source: Deloitte, 2022.

[7] "Cyber Risk capabilities in EMEA," Deloitte, 2022.

There is a wide variety of companies focusing on these specific areas, or combinations thereof. The focus shifts between the three stages. During the pandemic, most threats emerged from the inability to secure work-from-home activities. After solving mostly hardware-protection issues, the focus then shifted toward vigilance in a hybrid-work environment, where the resilience aspects receive more attention along the way. This translates to growth numbers for specifically focused cybersecurity software providers in the respective areas. There is also a focus on industries. Specialised finance and healthcare cybersecurity software providers have emerged more over the last couple of years. They tailor solutions to the most common threats for those specific industries.

The second approach: integrate data into portfolio management via integrated risk analytics

This approach involves attempting to integrate cybersecurity in a portfolio management context. In this case, we screen our holdings based on their cyber readiness. At this stage, that screening focuses mostly on the preventive aspects described above, by means of screening the company's basic cyber hygiene. It is by no means a complete picture of the threat landscape, nor a prediction tool for actual cyber hacks, but it is a strong starting point to create an evidence-based profile.

This solution comes from the insurance sector, where risk measures have been used for a couple of years to underwrite cybersecurity insurance. Whenever a company wants to be insured, it first needs to go through a basic hygiene screening. If it meets the minimum threshold, a deeper dive determines the appropriate premium and the company gets insured against cybersecurity risks. If the company does not live up to minimum cybersecurity standards, it will not be insured. We have taken this binary point-in-time approach to set up a database where we test these minimum requirements through time and track changes for our portfolio companies based on the "Known exploited vulnerabilities catalog", which is continuously updated by the US Government's Cybersecurity & Infrastructure Security Agency.[8] We then monitor those signals and take it a step further with the help of our engagement team. Whenever a cyber risk is identified, we contact the specific company and ask for an explanation on the evidence-based data we gathered. If the company has an explanation, we document these and monitor if the problem is resolved. If the company is unaware of the risks and not willing to take any action, we would rate cybersecurity risks as material and use that input in our portfolio positioning process.

A list of engagement questions can be found below. The main benefit of this approach is that we can combine evidence-based information with qualitative inputs. We can then objectively test the company's response in the months after our engagement to see if they are resolving the issue. By monitoring the behavior over a long period, we can get an accurate picture of cybersecurity integration into our portfolio holdings. This approach works not only for our equity holdings, but also for our exposure in private companies, convertibles and fixed income portfolios. The assessment is based on IP addresses and is therefore independent of asset class.

FIG 6. THE FOUR PILLARS OF CYBERSECURITY ENGAGEMENT

GOVERNANCE AND OVERSIGHT	POLICY STRUCTURE	REPORTING	TRAINING

GOVERNANCE AND OVERSIGHT

- What is the governance structure that underpins cybersecurity?
- What is the process for the identification, management and mitigation of risks from cybersecurity threats?
- Is cybersecurity part of the business strategy, financial planning and capital allocation?
- What is the role of the board in managing cybersecurity risks and implementing policies, procedures and strategies?
- Can the board demonstrate its effectiveness in cyber-related matters?
- Does the company identify a named person at a senior management or executive committee level as well as a non-executive director with overall responsibility for information management and cybersecurity?
- Is the board or is there a separate board committee responsible for cybersecurity issues?
- Does the company communicate cyber risks to the board (and how, by whom and how often)? What does the board do with the information?
- Describe how the (chief) risk officer and the (chief) operating officer are involved in cyber risk.
- How is cybersecurity included in the work of the audit committee?
- Does the nomination committee include cybersecurity as a standard skill needed for board refreshment/succession planning policies?
- Do remuneration policies for executives include cybersecurity metrics?
- Is training on cybersecurity provided to the board?
- Can you describe the extent to which cyber incidents have led to a change in company policy/process?

[8] CISA (2022).

POLICY STRUCTURE

- Is the company's policy (policies) on cybersecurity publicly available?
- Is it part of your general ESG reporting?
- If so, how have you integrated it into ESG?
- How often is the policy updated?
- Can you specify links between incidents and policy updates?
- Does M&A process/due diligence include enhanced cyber assessments?
- How is your cybersecurity approach/hierarchy/policy and process applied and expected across your whole supply chain? Is the supply chain audited from this angle? If so, what are the annual results?

REPORTING

- Does the company publish a standalone cybersecurity report?
- Does the company include cyber-related information in the annual report?
- Does the company describe cybersecurity in its ESG/sustainability report?

For all of the above and/or any other type of existing reporting:

- Is there periodic reporting on cybersecurity incidents?
- Is the definition of cybersecurity incidents public?
- Have you developed a definition of what materiality means for cybersecurity? What is a material incident?
- What reporting is available on actions taken and remedial action?
- Has the company developed cybersecurity metrics? If so which ones? Are there specific targets linked to the metrics?
- If so, how did you reach them? How do you track them? Can you provide evidence of tracking and trajectory?
- For tracked metrics, have you identified functions or geographies that are more prone to attacks? If so, how is this being addressed?
- Does this reporting or lack of reporting on cybersecurity make a difference in terms of investment decision-making?
- Have you published a Code of Best Practice for cybersecurity/resilience for suppliers?
- Risk management reporting: is the company disclosing what the risk management components of the cybersecurity programme are? How is the company performing them? Is this being linked to the talent profile? How diverse are the security teams?
- Is the company disclosing the split between incidents that were detected by the company and those detected by third parties (i.e., regulators)?
- Have you received certifications and assessments from outside auditors validating your compliance with business, legal, contractual and regulatory requirements?

TRAINING

- Have all of your employees received training on cybersecurity?
- Do you conduct regular phishing exercises?
- What are the success rates of the exercises?
- How do you ensure the above?

Source: LOIM, 2022.

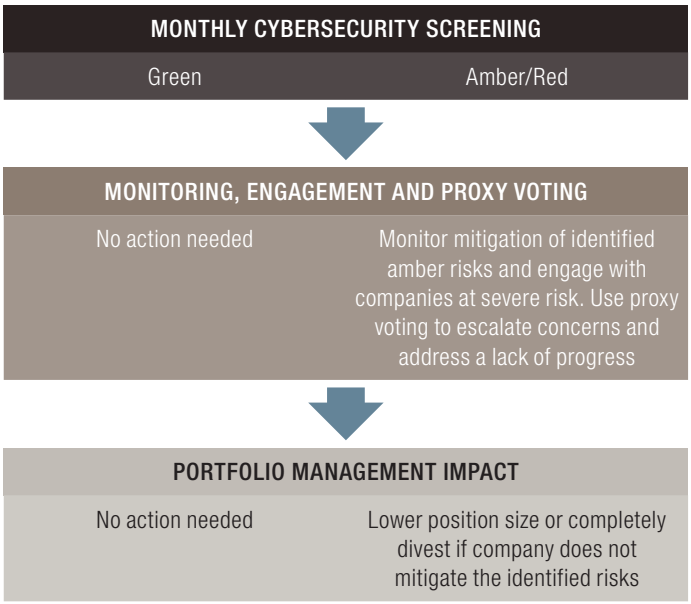
Our layered approach

Translating technical cybersecurity data into easy-to-understand outputs for investment managers and analysts is challenging. Therefore, our chosen approach has two layers. The first layer is a simplistic colour-coded output, which either indicates that there are no issues with known exploited vulnerabilities in the software and the basic hygiene check for the company came back positive, or that there is an issue.

The "issue" category is split in two parts: it could be something minor that requires monitoring, or a direct vulnerability that could lead to a breach, which we would classify as a top priority. This way, it is easy to screen large portfolios and to get a quick overview of cybersecurity risks. The second layer then goes deeper into the threats and their respective materiality. This involves discussion with the company, either by portfolio managers and financial analysts during, for example, quarterly calls with management, or by a specialised engagement team.

Continuous monitoring allows us to keep track of company responses to vulnerabilities and is evidence-based as opposed to questionnaire-based, which leaves ample room for interpretation. Through these steps, we hope to put cybersecurity top-of-mind for executives of companies we invest in, and in the process protect our clients from large breaches that could potentially impact portfolio returns.

FIG 7. CYBER RISK PROCESS FROM SCREENING TO PORTFOLIO MANAGEMENT IMPACT



Source: LOIM, 2022.

Conclusion

From the data we show in this report, it is clear that cybersecurity risks are having a substantial impact on businesses on a global scale. As investors, we need to find solutions to mitigate these risks. We think we have found a strong way to do so via the integration of cybersecurity insurance screening methodologies that we tailor to the needs of an asset manager. In addition to these screening tools, we also use our internal company engagement team to deepen our understanding of the cybersecurity threats for our portfolio holdings. By actively engaging with the portfolio holdings at risk of breaches, we hope to reduce the vulnerability of these companies to cybercrime.

We do not have a perfect prediction model for which companies will be attacked, but we do know which ones are more vulnerable. We also know which companies are best prepared for the unfortunate event of a breach. This information is integrated across asset teams in the portfolio management process and ultimately serves as one of the inputs to optimise the risk-return trade-off for our different mandates.

What we have built at present is only the beginning, and we hope to learn a lot during the years ahead and to be able to integrate more detailed information along the way. The more asset managers pay attention to cybersecurity risks, the more corporations, clients, suppliers and wider stakeholders will pay attention to it. In turn, this should benefit society as a whole.

IMPORTANT INFORMATION

For professional investor use only.
This document is issued by Lombard Odier Asset Management (Europe) Limited, authorised and regulated by the Financial Conduct Authority (the "FCA"), and entered on the FCA register with registration number 515393.
Lombard Odier Investment Managers ("LOIM") is a trade name.
This document is provided for information purposes only and does not constitute an offer or a recommendation to purchase or sell any security or service. It is not intended for distribution, publication, or use in any jurisdiction where such distribution, publication, or use would be unlawful. This material does not contain personalized recommendations or advice and is not intended to substitute any professional advice on investment in financial products. Before entering into any transaction, an investor should consider carefully the suitability of a transaction to his/her particular circumstances and, where necessary, obtain independent professional advice in respect of risks, as well as any legal, regulatory, credit, tax, and accounting consequences. This document is the property of LOIM and is addressed to its recipient exclusively for their personal use. It may not be reproduced (in whole or in part), transmitted, modified, or used for any other purpose without the prior written permission of LOIM. This material contains the opinions of LOIM, as at the date of issue.
Neither this document nor any copy thereof may be sent, taken into, or distributed in the United States of America, any of its territories or possessions or areas subject to its jurisdiction, or to or for the benefit of a United States Person. For this purpose, the term "United States Person" shall mean any citizen, national or resident of the United States of America, partnership organized or existing in any state, territory or possession of the United States of America, a corporation organized under the laws of the United States or of any state, territory or possession thereof, or any estate or trust that is subject to United States Federal income tax regardless of the source of its income.
Source of the figures: Unless otherwise stated, figures are prepared by LOIM.
Although certain information has been obtained from public sources believed to be reliable, without independent verification, we cannot guarantee its accuracy or the completeness of all information available from public sources. Views and opinions expressed are for informational purposes only and do not constitute a recommendation by LOIM to buy, sell or hold any security. Views and opinions are current as of the date of this presentation and may be subject to change. They should not be construed as investment advice.
No part of this material may be (i) copied, photocopied or duplicated in any form, by any means, or (ii) distributed to any person that is not an employee, officer, director, or authorised agent of the recipient, without Lombard Odier Asset Management (Europe) Limited prior consent. In the United Kingdom, this material is a marketing material and has been approved by Lombard Odier Asset Management (Europe) Limited which is authorized and regulated by the FCA.
©2022 Lombard Odier IM. All rights reserved.