

# CYBERSECURITY RISK & RESILIENCE

**Guidance for investors –**  
A joint report by Railpen and  
Royal London Asset Management

RAILPEN

  
**ROYAL  
LONDON**  
ASSET MANAGEMENT



# CONTENTS

Authors and acknowledgements .....	3
Executive summary .....	5
Introduction .....	6
Why should investors care about cybersecurity? .....	8
What should investors expect of portfolio companies? .....	16
What can investors do? .....	22
References .....	29

# AUTHORS AND ACKNOWLEDGEMENTS

This report has been prepared by **Georgina Chiu** (Royal London Asset Management), **Sophie Harris** (Railpen) and **Jasmine Porter** (Railpen).

Technical review was conducted by **Shaun Roberts** (Railpen), **Bryan Kavanagh** (Railpen), and **Hilary Loftus** (Royal London).

We would like to thank the following colleagues for their valuable feedback and input:

- **Caroline Escott** (Railpen)
- **Becks Goodman** (Railpen)
- **Paul O'Donnell** (Railpen)
- **Carlota Garcia-Manas** (Royal London Asset Management)
- **Charles Stott** (Royal London Asset Management)

We would also like to thank the members of the Cybersecurity Coalition – Nest, USS, Border to Coast, and Brunel Pension Partnership – for their support.

## RAILPEN

Railpen is entrusted, on behalf of the Trustee, with the safekeeping and investment of around £34 billion in assets, and providing support for 350,000 members of the railways pension schemes.

The schemes consist of over 100 different employers and contain a mixture of open and closed DB sections, DC and hybrid arrangements. The Railways Pension Scheme, in particular, is one of the UK's largest, most complex and longest-established pension funds.

The Trustee's mission is to pay members' pensions securely, affordably and sustainably. Railpen supports the Trustee in delivering this through our own purpose of securing our members' future. We recognise that members and employers trust us with a significant responsibility, and that the decisions and actions we take affect members' future lives and wellbeing. We're proud of this responsibility, take it seriously and are committed to and passionate about improving the lives of members.

We have long investment horizons and plan into the next century and beyond. The management of long-term risk and opportunity is therefore fundamental to our investment approach. This includes our long-standing work on sustainable ownership – incorporating our ESG Integration, Active Ownership and Climate workstreams into the investment process.

Find out more at [www.railpen.com](http://www.railpen.com)





## At Royal London Asset Management, we do things a little differently.

We take a distinct approach to active management. As an integral part of customer-owned mutual Royal London, we're free from short-term shareholder demands. Instead, we put our clients at the heart of what we do, using a longer-term perspective to generate investment returns.

It's a different pressure to perform and we thrive on it. As active long-term investors, we create solutions with the right balance of return and risk. Our consistent track record across asset classes speaks for itself.

We are independent, responsible investors. Entrusted with other people's money, we embrace the influence we have as stewards of our clients' capital, for the mutual benefit of our clients and wider society.

We are dedicated to delivering for our clients around the world. Building a better future, together.

**It's asset management excellence, with a longer-term perspective.**

Find out more at [www.rlam.com](http://www.rlam.com)

Royal London Asset Management is one of the UK's leading asset management companies<sup>1</sup>, managing £169.5 billion of assets under management, as at June 2024, on behalf of a wide range of clients, including Royal London Mutual Insurance Society, corporate pension schemes, local authorities, insurance companies, endowments, charities, universities, and various financial intermediaries.

<sup>1</sup> Based on UK Total sales. The Pridham Report, 2021 – 2023.

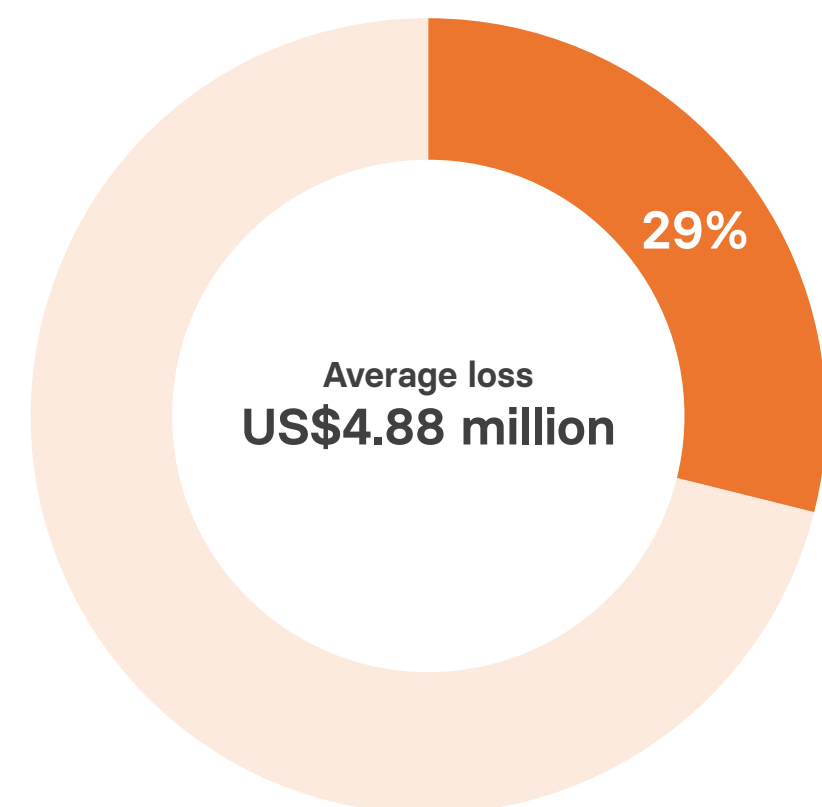
Past performance is not a guide to future performance.



# EXECUTIVE SUMMARY

## Cybersecurity is a growing and financially material risk to investment portfolios.

The World Economic Forum 2024 Outlook reported that 29% of organisations stated that they had been materially affected by a cyber incident in the past 12 months<sup>1</sup>. The average loss associated with a data breach and recovery process was estimated to be US\$4.88 million in 2023<sup>2</sup>.



■ Percentage of organisations materially affected by cyber incident in the past 12 months

In 2019, Railpen joined forces with Nest on the issues around cyber and data security. This resulted in a joint report: **'Why UK pension funds should consider cyber and data security in their investment approach'**. Soon after, Royal London Asset Management set up a Cybersecurity Coalition, comprising of investors including Railpen, Nest, USS, Border to Coast, and Brunel Pension Partnership, in an effort to address the systemic risks around this thematic stewardship issue, which has seen us engaging with portfolio companies and participating in policy advocacy.

This new report by Railpen and Royal London Asset Management provides an evidence-based perspective on the financial materiality and threat landscape of cybersecurity risk, as well as practical guidance for investors around engagement with portfolio companies on this topic. For the purposes of this report, the term 'investors' covers asset owners and asset managers.

**Cybersecurity Risk & Resilience: Guidance for investors** brings together the unique perspectives of Railpen, an asset owner, and Royal London Asset Management, an asset manager, based on our experience over the last five years.

This report seeks to answer the following questions:

1. Why should investors care about cybersecurity?
2. What should investors expect of portfolio companies?
3. What can investors do?

Based on the evidence we present in this report and our experience, we invite investors to consider the following steps:

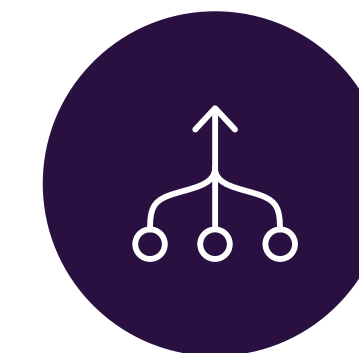
- Recognise the financial materiality of cybersecurity to their portfolios.
- Use the expectations outlined in this report as a tool to assess companies' baseline approach to cybersecurity and measure their progress towards best practice. The expectations are based on our four pillars – explained later in this report (see right).
- Identify and engage with companies that face high-risk exposure, using sector-specific vulnerabilities as a lens for screening and our recommended questions to initiate dialogue.
- Participate in policy advocacy on cybersecurity, as a supportive regulatory environment will enable improved alignment between company disclosures and investors' expectations<sup>a</sup>.

<sup>a</sup> While these recommendations can be applied more broadly, the report focuses on large publicly-listed companies in major markets that most investors are exposed to: the UK, the US and the EU.



### Governance

Robust board oversight is essential for implementing effective cybersecurity practices.



### Supply chain and mergers & acquisitions (M&A)

Comprehensive due diligence and proactive risk management of external parties are critical.



### Processes, culture and training

Fostering a resilient culture is fundamental, supported by strong vulnerability management, testing and certifications.



### Collaboration

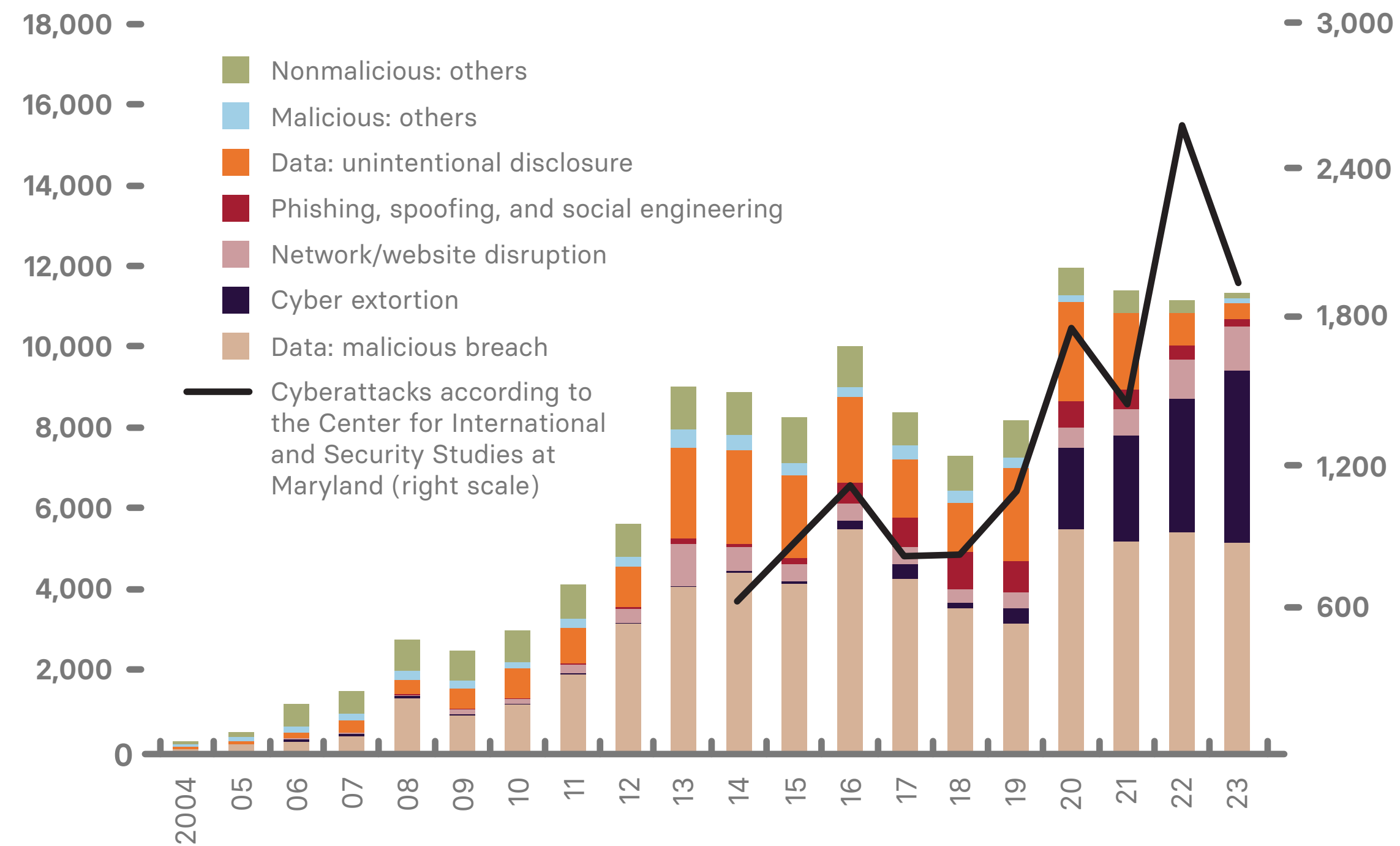
Working with peers and government bodies is crucial to enhancing cybersecurity standards.

# INTRODUCTION

Since the publication of Railpen’s and Nest’s report in 2019, cybersecurity risk across investment portfolios has continued to grow.

The number and severity of cyberattacks have increased dramatically in recent years, posing significant threats to the financial performance and stability of companies across most sectors. According to the International Monetary Fund (IMF), cyber incidents with malicious intent have almost doubled since the Covid-19 pandemic<sup>3</sup> (see Figure 1). The World Economic Forum 2024 Outlook reported that 29% of organisations stated that they had been materially affected by a cyber incident in the past 12 months<sup>4</sup>.

Figure 1: Global number of cyber incidents 2004-2023



Source: IMF (2024), Global Financial Stability Report

## What is cybersecurity?

According to the UK National Cyber Security Centre, cybersecurity is how individuals and organisations reduce the risk of cyberattacks.

Cybersecurity’s core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access – both online and at work – from theft or damage. It’s also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.

Source: [ncsc.gov.uk/section/about-ncsc/what-is-cyber-security](https://ncsc.gov.uk/section/about-ncsc/what-is-cyber-security)



Cyberattacks have also become more costly, as the risk of extreme losses – at least as large as US\$2.5 billion – has increased, sometimes putting firms at risk of insolvency<sup>5</sup>. Global cybercrime costs are expected to surge by 15% throughout 2024 to £8.2 trillion by the end of 2025, but the actual extent of the damage is likely to be much higher as many attacks go undetected or unreported<sup>6</sup>. Indeed, Keeper Security’s 2022 US cybersecurity census report found that 48% of US Information Technology (IT) leaders have been aware of a cyberattack but not reported it<sup>7</sup>.

Evolving threat drivers, such as geopolitics, artificial intelligence (AI), skills shortages and supply chain vulnerabilities, reinforce the need for portfolio companies to prepare for ‘when’ a cybersecurity incident will occur, rather than ‘if’. Company leaders are increasingly aware of this. In the UK, 98% of large corporations report that cybersecurity is a high priority for their senior management<sup>8</sup>. On a global scale, 70% of Chief Information Security Officers (CISOs) and 73% of board members think that they are likely to face a material cyberattack over the next 12 months<sup>9</sup>.

Concerningly, there appears to be a disconnect between leaders’ awareness and preparedness. Around 40% of surveyed CISOs concede that their organisation is unprepared to cope with a targeted cyberattack<sup>10</sup>. Should cybersecurity risk crystallise, companies face substantial disruption and an often lengthy path to recovery. This disruption can be coupled with the increased cost of insurance premia, lenders raising the company’s cost of debt, and shareholders filing litigation. Beyond these direct losses, the impacts of a cybersecurity incident can ripple throughout a system due to technological interdependencies. Such ripples can lead to breakdowns in critical healthcare, transport, and banking systems, which will negatively impact the portfolios of ‘universal owners’.

Due to the potential systemic impacts of cyberattacks, it is unsurprising that regulators are paying more attention to companies’ risk controls ([see page 12](#)) and that corporate investment in cybersecurity is rising. Research by The Ponemon Institute found that 59% of surveyed US companies increased their cybersecurity budgets year-on-year<sup>11</sup>. On a relative basis, Moody’s found that companies have doubled the proportion of their technology budgets dedicated to cybersecurity since 2019, rising to an average of 9% in 2023<sup>12</sup>. However, it’s important to note that higher spending is not always indicative of better preparedness, so investors should look beyond headline figures.

### What is systemic risk?

According to the WEF, systemic risk refers to the possibility that a single event or development may trigger widespread failures and negative impacts spanning multiple organisations, sectors, and/or nations.

Source: [weforum.org/docs/WEF\\_GFC\\_Cybersecurity\\_2022.pdf](https://weforum.org/docs/WEF_GFC_Cybersecurity_2022.pdf)

The increasing number, cost, and threat drivers of cybersecurity incidents, coupled with a disconnect between awareness of, spending on and preparedness for this risk at a company level, is leading to growing cybersecurity risk across portfolios. **We believe cybersecurity needs more attention, particularly due to its systemic implications, and we invite investors to take action.**

The Cybersecurity Coalition’s expectations draw upon a unique collaboration between technical experts, asset owners, and asset managers. They provide investors with a tool to elevate stewardship from reactive engagement after a cyber incident to proactive dialogue on resilience. Our approach, which has been tested over multiple years, provides the basis for engagement with vulnerable companies, while also participating in policy advocacy to support an effective system-wide response to cybersecurity risks. For further information on our recommended steps, continue reading to the final section of this report: **‘What can investors do’**.



“We are delighted that Royal London Asset Management and Railpen have continued this important research and developed updated guidance for investors. In a world of fast digital transformation driven by AI, cybersecurity risk continues to grow for all companies and for us as investors. We expect corporate boards to be adequately prepared for cyberattacks with operational resilience at the heart of a cybersecurity strategy. We will use the guidance to enhance our engagements with companies to help protect our 13 million members from this systemic risk.”

**Diandra Soobiah, Director of Responsible Investment, Nest**

“Cyber incidents will continue, with increasing frequency and sophistication. Investors can only protect value by understanding the risk factors, governance and strategy, and by knowing what questions to ask. This collaborative engagement has built on our understanding and provided valuable insights on set expectations.”

**Faith Ward, Chief Responsible Investment Officer, Brunel Pension Partnership**



# WHY SHOULD INVESTORS CARE ABOUT CYBERSECURITY?

## Defining the risk

There is no single definition of a cybersecurity incident, but the US National Institute of Standards and Technology (NIST) describes it as “a cybersecurity event that has been determined to have an impact on the organisation prompting the need for response and recovery”<sup>13</sup>. Impacts include the jeopardisation of information or an information system’s integrity, confidentiality, or availability; or the violation of regulation or internal security policies and procedures. Such incidents are varied, arising as a result of human error, IT failures, and malicious actors.

Malicious actors were estimated to have caused 55% of data breaches between March 2023 and February 2024<sup>14</sup>. Of these breaches, the EU Agency for Cybersecurity identified ransomware and Denial of Service (DoS) as the most commonly reported threats<sup>15</sup>.

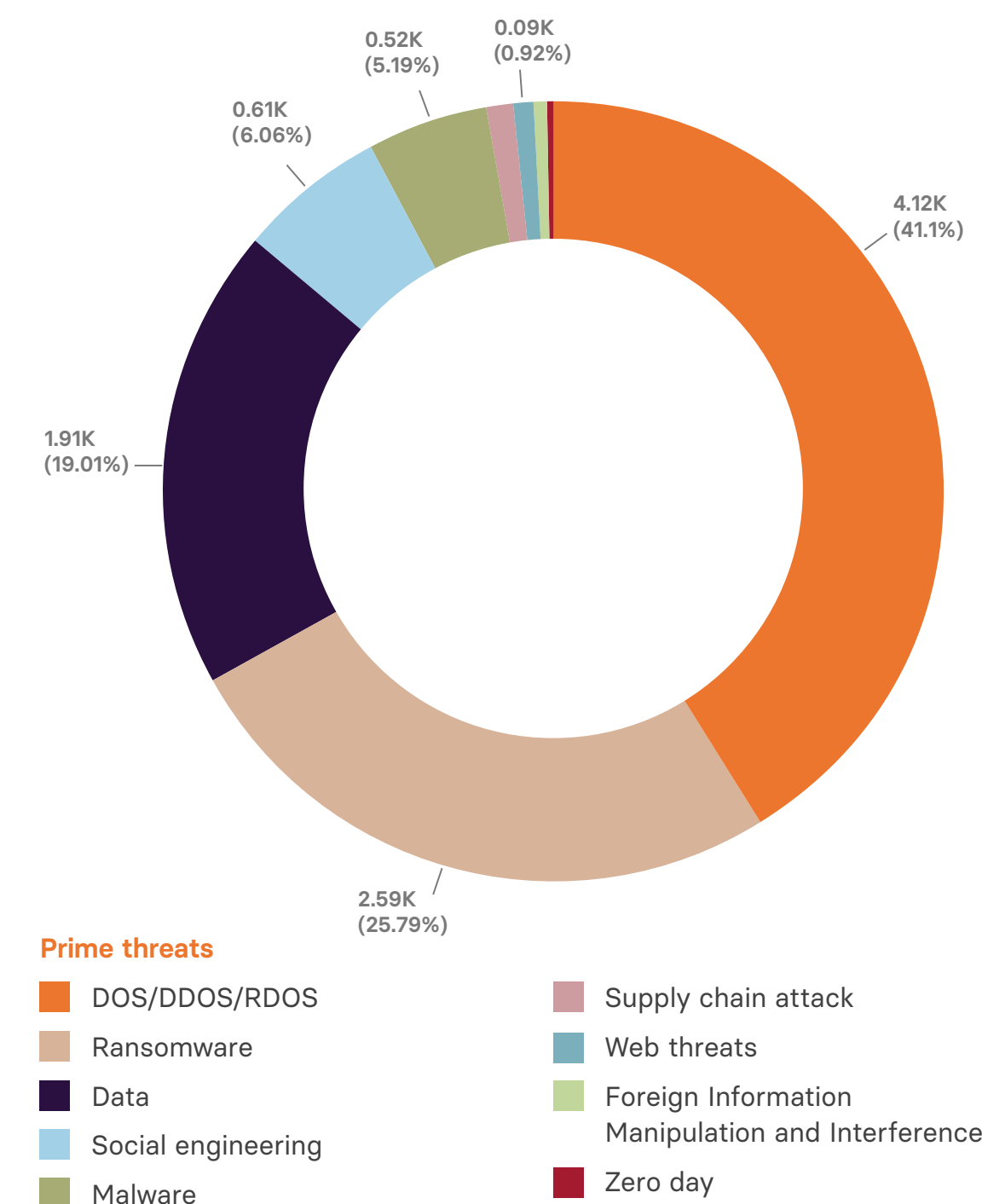
Ransomware is a type of malicious attack where attackers encrypt an organisation’s data and demand payment to restore access. In some instances, attackers may also steal an organisation’s information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public<sup>16</sup>. If the victim organisation refuses to pay the ransom demand, threat actors will sometimes perform a distributed denial of service attack (DDoS) against the organisation’s web application. This is an attempt to increase pressure to make payment by making the web application unavailable. This combination of attack methods is known as a triple extortion ransomware<sup>17</sup>.

Figure 2: Prime cybersecurity threats



Source: European Union Agency for Cybersecurity (2023), ENISA Threat Landscape 2023

Figure 3: Breakdown of analysed incidents by threat type (July 2002-June 2023)



Source: European Union Agency for Cybersecurity (2023), ENISA Threat Landscape 2024



## Financial materiality

When cybersecurity risk crystallises, companies face substantial disruption and often a lengthy path to recovery. According to IBM’s Cost of a Data Breach Report 2024, 78% of organisations that had achieved full operational recovery post-breach said that it took longer than 100 days, and 35% took longer than 150 days<sup>18</sup>. The average loss associated with a data breach and this recovery process was estimated to be US\$4.88 million in 2023<sup>19</sup>. As a coalition focused on cybersecurity, we recognise the substantial damage such threats can cause to our portfolio companies. This in turn can affect the value of scheme members’ savings and clients’ investments.



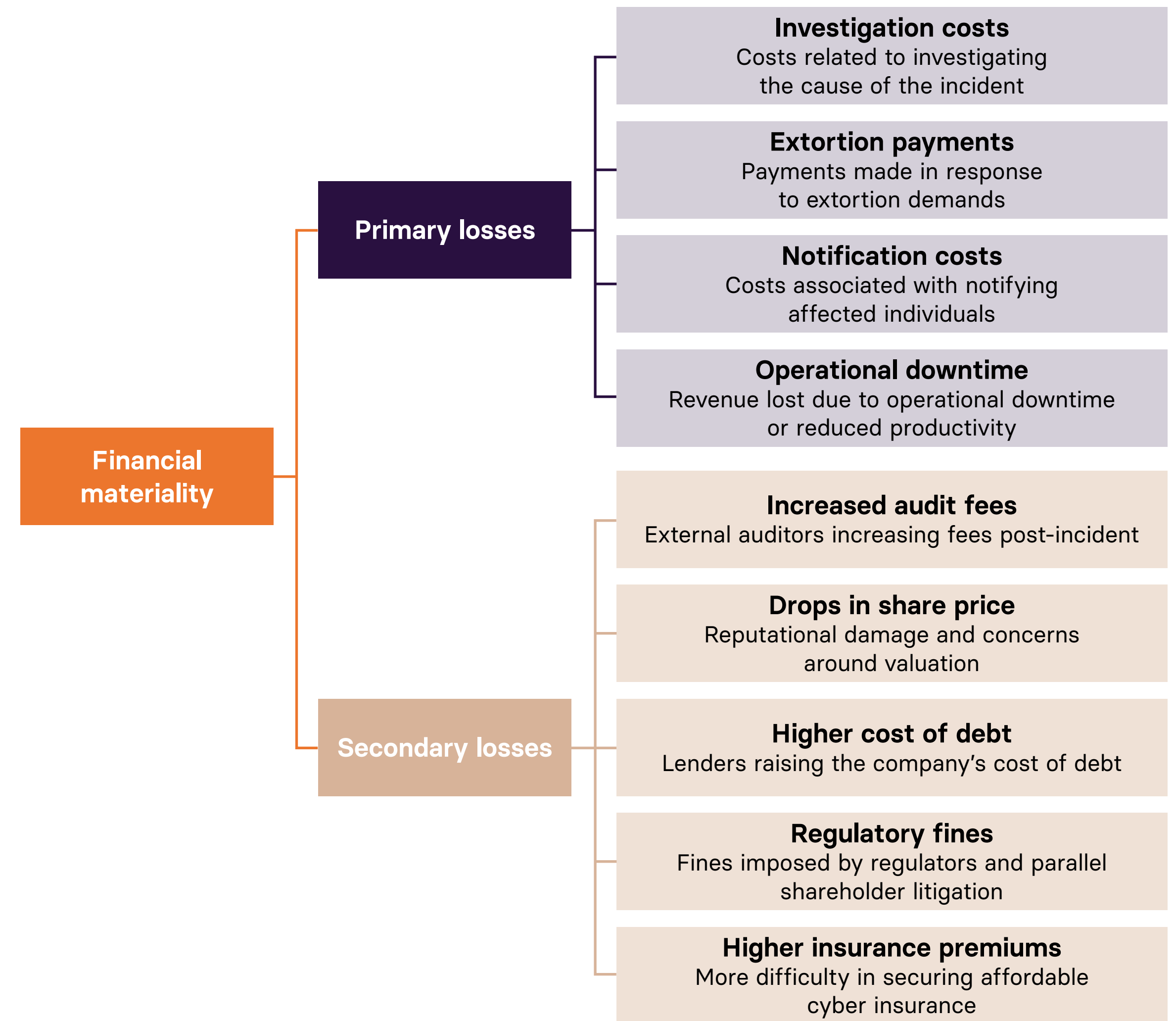
IBM found that **78%** of organisations took longer than **100 days** to achieve full operational recovery, and **35%** took longer than **150 days**



The average loss associated with a data breach and this recovery process was estimated to be **US\$4.88 million**

Contributors to cybersecurity loss can be classified as ‘primary’ or ‘secondary’<sup>20</sup>. Primary losses are incurred as a direct result of the incident, including costs related to investigating the cause, responding to extortion, and notifying affected individuals. Revenue may also be lost through operational downtime or reduced productivity due to diverted resource and attention. Beyond these immediate costs, poor cybersecurity risk management can have a sustained effect on the valuation of a company<sup>21</sup>. Secondary losses may be incurred through the actions of affected stakeholders, such as external auditors increasing fees post-incident, lenders raising the company’s cost of debt, and regulators imposing fines.

Figure 4: Primary and secondary losses from cybersecurity incidents



### Extortion payments

Most ransomware attacks are the result of poor cyber hygiene rather than sophisticated techniques<sup>22</sup>. Nonetheless, the cost can be significant: "...a seven-figure or more ransom sum is now the norm"<sup>23</sup>. British IT Security company, Sophos, estimates that the mean and median ransom payment rose to US\$3.96 million and US\$2 million in 2023, respectively<sup>24</sup>. These payments were primarily funded by the affected organisation, covering 40% of the cost on average<sup>25</sup>. However, the liability can be partly transferred to others, as 23% of ransom costs were reported to be paid by insurance providers<sup>26</sup>.

Ransomware attackers apply pressure on their targets by denying access to critical systems and/or threatening to leak stolen data. When attackers use encryption, companies generally recover the data by paying the ransom to obtain the decryption key (in 56% of cases) and using backup systems (in 68% of cases)<sup>27</sup>. To increase the likelihood of payment, attackers will often extend their focus to companies' backup systems. Despite movements to immutable cloud-hosted systems, over half of reported attempts to compromise backups were successful in 2023<sup>28</sup>. Affected companies were almost twice as likely to pay the ransom and their recovery costs post-payment were around eight times higher<sup>29</sup>.

### Business disruption

When data is breached, systems that are reliant upon it are likely to be disrupted. As a result, cybersecurity incidents often cause unplanned operational downtime and reduce productivity. The financial impact of downtime vary by cause, systems affected, and the sector in which the company operates (see page 23). However, the average cost of unplanned IT downtime has been estimated to range from US\$5,600 to US\$23,750 per minute<sup>30</sup>. More recently, IBM found that lost business costs totalled an average of US\$1.47 million for breached companies<sup>31</sup>.

The average cost of unplanned IT downtime ranges from **US\$5,600** to **US\$23,750** per minute

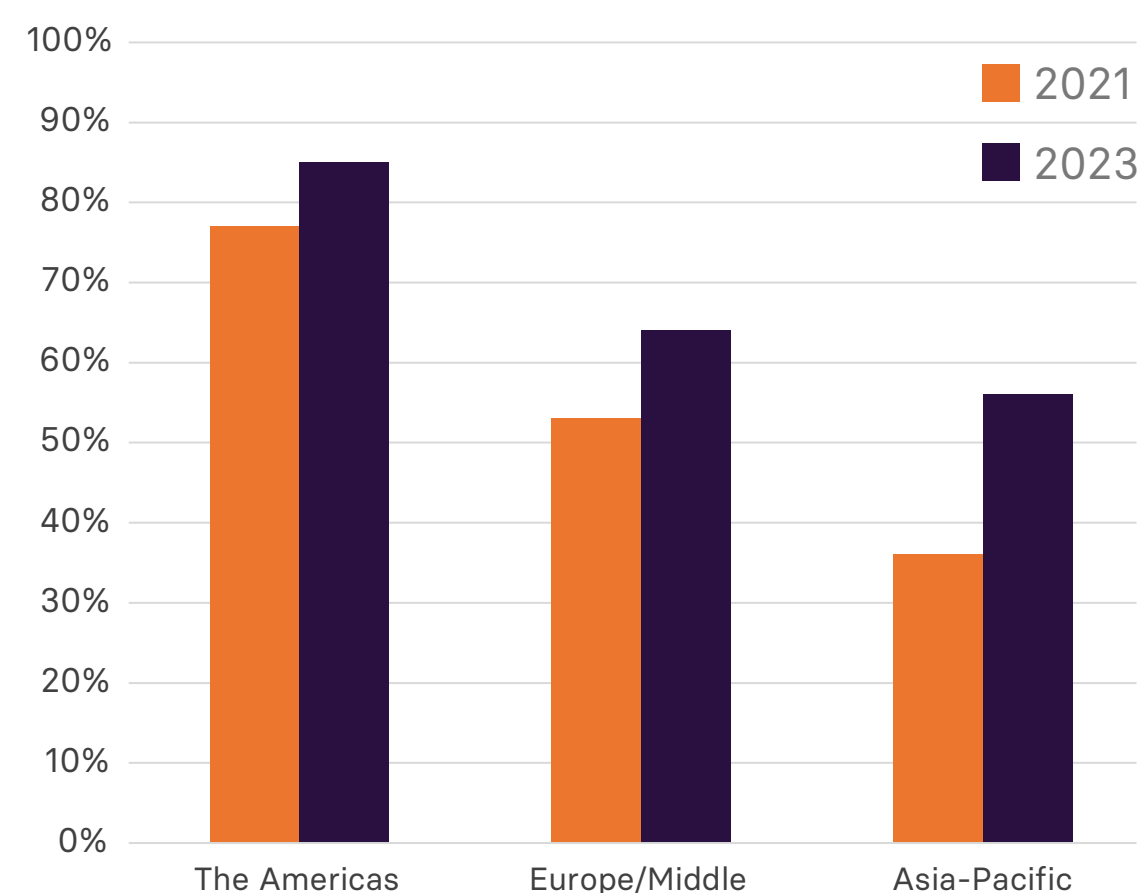
IBM found that lost business costs totalled an average of **US\$1.47 million** for breached companies

Following initial efforts to restore systems, operations can face further disruption due to the diversion of employees' attention. Such attention may be focused on the remediation of customers and the establishing of new controls to manage the potential for future incidents.

### Higher insurance premiums

Cybersecurity risk is increasingly being transferred to insurers. An estimated US\$12 billion of gross premiums were written in 2023<sup>32</sup>. Since 2021, the share of companies with cybersecurity insurance has reportedly grown by 8% in the Americas, 11% in EMEA, and 20% in APAC<sup>33</sup>. In parallel, the importance placed on cyber insurance is rising. A recent survey conducted with US-based practitioners found that the purchase of cyber insurance was considered to be the second most important cybersecurity governance activity (46% of respondents)<sup>34</sup>.

Figure 5: Percentage of respondents to Moody's Cybersecurity Survey that reported carrying standalone cyber insurance



Source: Moody's (2023), 2023 Cybersecurity Survey Highlights

Despite this, around half of respondents said that it was highly difficult to purchase cyber insurance because of the prerequisites for coverage<sup>35</sup>. Compounding the challenge, insured companies that make claims on a frequent basis, or for an incident that resulted in significant losses, are likely to attract a higher premium.

To mitigate the risks of inaccessible or very costly insurance, companies can raise their "security posture"<sup>36</sup>.

High security posture is characterised by the following controls, which are aligned to the investor expectations set out in this guidance:

- The presence of a dedicated CISO
- Appropriate resourcing
- Strategic investment
- Employee training programmes
- Regular vulnerability audits
- A comprehensive approach to third-party risks
- Participation in threat-sharing programs.

Insurers recognise that financially material events can be intercepted early when companies proactively invest in these controls<sup>37</sup>. Global insurance group, Howden, notes: "Effectively mandating the implementation of controls such as multifactor authentication (MFA) and backups has had a huge impact in improving the underlying risk of cyber-insurance portfolios"<sup>38</sup>.

## Drop in share price

Multiple studies have shown that significant cybersecurity incidents have been found to cause material drops in share prices. In 2023, security research firm, Comparitech, analysed 118 companies listed on the NYSE that have experienced data breaches<sup>39</sup>. On average, breached companies underperformed the NASDAQ by -3.2% in the six months following the disclosure of an incident. Similarly, Moody's found that cyber incidents at 1,542 listed companies resulted in abnormal equity returns, ranging from -0.3% to -5.3% over a 12-month period<sup>40</sup>. By comparison, the IMF only observed an average 0.1 to 0.2% fall in share prices following malicious cybersecurity incidents across 644 listed companies, albeit market reactions were much stronger in relation to small firms<sup>41</sup>.

Evidence suggests that a company's ability to restore the confidence of investors and customers can limit the downside of a cybersecurity incident in the short term, and even contribute to an improved reputation over the long term<sup>42</sup>. The Ponemon Institute found that companies with high security posture recovered their share prices within an average of seven days, whereas those with low posture experienced a decline for more than 90 days<sup>43</sup>.



In 2023 Comparitech analysed **118 companies** that have experienced data breaches



Breached companies underperformed the NASDAQ by **-3.2%** on average in the six months following the disclosure of an incident.

## Elevated cost of debt

A cybersecurity incident can signal to lenders that a borrower is less likely to fulfil its financial obligations, in part due to unplanned investment in internal controls. Reflecting this negative signal, a borrower's credit rating may decrease. For example, Moody's began incorporating cybersecurity risk into existing credit ratings in 2018 and has consequently shifted ratings in 19 instances for 10 debt issuers<sup>44</sup>. The agency notes: "Cash-strapped debt issuers with low liquidity and high leverage are more susceptible to the negative credit effects of cyber incidents"<sup>45</sup>. Highly diversified companies with larger and more liquid financial resources are better insulated, but necessary cybersecurity investments can strain an underprepared company's free cash flow for many years.

A company's cost of debt is expected to rise when its credit rating is downgraded and additional credit monitoring services are required. Based on a sample of 290 breached companies, research found that affected firms' cost of debt was 30 basis points higher on average post-breach than unaffected firms between 2005 and 2018<sup>46</sup>. The impact was more pronounced for borrowers with poorer credit ratings pre-breach, less investment in control systems, and significant changes in cash flow expectations post-breach. The magnitude of this cost increase is similar when companies receive a modified audit opinion (17 basis points) or are found to have material weaknesses in internal controls (28 basis points)<sup>47</sup>.


## Increased audit fees


As mentioned cybersecurity incidents can be indicative of broader deficiencies in internal controls. External auditors are responsible for detecting such material weaknesses in relation to information reporting, and evaluating the impact of an incident upon a company's financial statements in order to determine their opinion. Therefore, companies are likely to face increased auditor scrutiny after a cybersecurity incident occurs. To mitigate the higher level of audit risk, external auditors use additional resource to gather evidence and conduct testing<sup>48</sup>. As a result of this additional effort, research in 2019 found that breached firms are charged approximately 12% higher audit fees in the year of the incident<sup>49 b</sup>.

<sup>b</sup> While increased audit fees may impact a company, we note evidence on the benefits to investors of high quality audits. More detail can be found in Railpen's Acting on Audit Report, which is available at [cdn-suk-railpencom-live-001.azureedge.net/media/media/ycodtbv4/railpen-acting-on-audit-report.pdf](https://cdn.suk-railpencom-live-001.azureedge.net/media/media/ycodtbv4/railpen-acting-on-audit-report.pdf).

### Regulatory action

When risk management fails to prevent a data breach, the EU General Data Protection Regulation (GDPR) and UK GDPR require companies to report notifiable incidents within 72 hours of becoming aware of them. Failure to do so can result in fines as high as €20 million or 4% of the company's worldwide annual revenue in the EU, and £17.5 million or 4% of the company's global turnover in the UK.

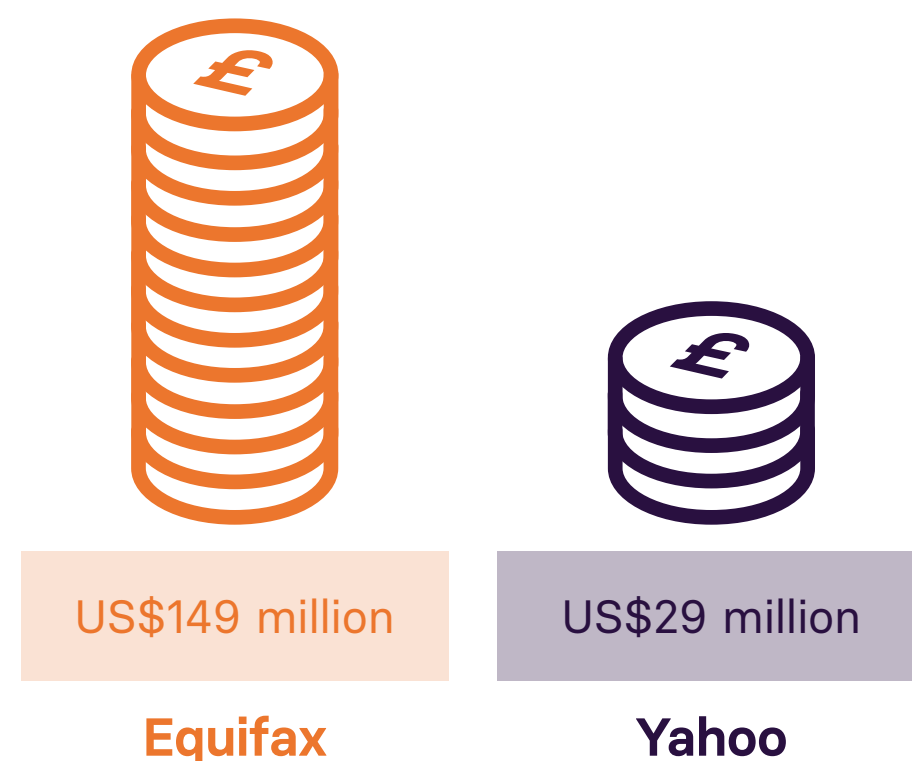
 **GDPR (EU/UK): Report notifiable incidents within 72 hours.**

Failure to report on time (EU): Fines up to **€20m** or **4%** of company turnover. 

Failure to report on time (UK): Fines up to **£17.5m** or **4%** of company turnover. 

Where a firm is regulated by the UK Financial Conduct Authority or the Prudential Regulation Authority, it may face further sanctions if it is unable to evidence appropriate controls in line with its regulatory obligations. In the US, the Securities and Exchange Commission (SEC) now requires publicly-traded companies to report 'material' incidents within four business days of determining their materiality. A wilful violation of the SEC's requirement can result in a penalty of US\$5 million for individuals and US\$25 million for corporations.

More stringent disclosure requirements have provided further opportunities for shareholder litigation in the US, as it can be challenging to determine whether an incident reaches the 'material' threshold for disclosure. Materiality in this context can depend upon harm caused to a company's reputation, financial performance, vendor and customer relations, and potential regulatory action<sup>50</sup>. If shareholders disagree with a company's determination, they can assert that the information disclosed is insufficient or misleading. Additionally, shareholders can argue that directors have breached their fiduciary duty by failing to adequately oversee cybersecurity risk<sup>51</sup>. While these kinds of lawsuits have largely been dismissed, notable settlements include Equifax (US\$149 million)<sup>52</sup> and Yahoo! (US\$29 million)<sup>53</sup>.



### Key cybersecurity regulation in the EU, US & UK during 2024

The EU has developed a holistic web of regulation for different aspects of the cybersecurity environment including companies, information and communication technology (ICT) products, managed security-service providers and specific sectors:

- The Network Information and Security 2 (NIS2) Directive, in force from October 2024, is a pivotal EU-wide legislation. It's focused on cybersecurity for companies, introducing legal measures to improve the overall cybersecurity level in the EU by enforcing stricter reporting requirements and more rigorous security measures for important entities<sup>54</sup>. NIS2 is an updated version of the 2016 NIS Directive, and provides improved guidance and clarity on cybersecurity requirements by expanding the scope of essential and important entities, specifying management liabilities, outlining how controls should be carried out, increasing supply chain due diligence, and addressing how breaches should be reported<sup>55</sup>.
- The 2019 Cybersecurity Act complements the NIS Directive by giving ENISA – the European Union Agency for Cybersecurity – a permanent mandate and creating the EU cybersecurity certification framework for ICT products, processes and services<sup>56</sup>. An amendment to the Cybersecurity Act was proposed in April 2023 which would

expand the adoption of European cybersecurity certification schemes to 'managed security services'<sup>c</sup> covering areas such as incident response, penetration testing, and security audits<sup>57</sup>. The wording of the amendment mirrors language in the NIS2 Directive and therefore ensures consistency in the EU's cybersecurity strategy<sup>58</sup>.

- More recently, the EU is implementing sector-specific regulation with the Digital Operational Resilience Act (DORA), which has been adopted to define specific rules to enhance the resilience of the banking sector, and is being applied from 2025<sup>59</sup>.

Since 2022, both the US and UK have introduced national cybersecurity strategies:

- Reflecting the aim of the US to rebalance cybersecurity responsibility from customers to corporations, companies regulated by the SEC must now disclose how their board and executives oversee and manage material cybersecurity risks, alongside the relevant processes in place<sup>60</sup>.
- With more focus on awareness raising in the UK, a Cyber Governance Code of Practice was released for consultation in early 2024, which aims to support company leaders and boards in driving cyber resilience up the agenda<sup>61</sup>. Although the proposed actions will be voluntary, the UK Government has noted that they could pave the way for stronger measures, such as domestic regulation.

<sup>c</sup> Defined as "carrying out, or providing assistance for, activities relating to... customers' cybersecurity risk management"

## Horizon scanning: Threat drivers

In the evolving landscape of cybersecurity, investors must be vigilant of factors that drive and amplify threats to their portfolio companies. The WEF 2024 Global Cybersecurity Outlook highlights the following four considerations:

1. Supply chains and third parties
2. AI
3. Skills shortages
4. Geopolitics<sup>62</sup>

We can assess companies' readiness to face these threats by using the expectations of companies that are set out later on in this guidance ([see page 16](#)). For example, contagion risk in supply chains can be evaluated through third-party management strategies. Additionally, a company's employee training programmes and incident response plans can provide insight into its preparedness for AI-generated risks.

### 1. Supply chains and third parties

The interconnectedness of the cyber ecosystem means that third-party and supply chain considerations are crucial when assessing cybersecurity risks. In total, 53% of cyber leaders agree that a secure perimeter does not exist in their current ecosystem highlighting the need for a deep understanding of risks originating in supply chains<sup>63</sup>. Current company practices do not reflect this, with 71% of the smallest organisations by revenue not having been asked to prove their cyber posture by their supply chain partners in the past 12 months<sup>64</sup>. This is particularly concerning given the increasing

inequity between small and large organisations, with the smallest organisations being twice as likely to say they lack the cyber resilience they need to meet their operational requirements<sup>65</sup>.

This widening gap between organisations of different sizes is therefore not only an issue for the small organisations, as the interconnected cyber environment exposes larger companies to the vulnerabilities of smaller counterparts through their supply chains.

Systemic risks further compound supply chain and third-party vulnerabilities. Many organisations from different sectors rely on the same third-party software, thereby concentrating risks when this shared service provider faces a cyberattack. More than 90% of Russell 3000 firms have specific third-party technology providers in common and one-third of companies are utilising the same cloud services provider at the same specific location<sup>66</sup>. This concentration of risk could lead to systemic consequences.

Although the July 2024 tech outage caused by CrowdStrike was not due to a cyberattack, it demonstrates how many organisations rely on the same software and the wide-reaching consequences this has on society. As highlighted by a recent IBM report, business partner and software supply chain attacks account for 15% and 12% of attacks, respectively<sup>67</sup>. Another study by ISS, looking at incidents at Russell 3000 companies between 2021 and 2023, found that one-third of incidents involved a supplier or third-party relationship<sup>68</sup>. These types of incidents also tend to have a broader impact, as third-party incidents accounted for 60% of reported incidents impacting 100,000 or more individuals<sup>69</sup>.



## 2. AI

Generative AI is predicted to have the most significant impact on cybersecurity in the next two years<sup>70</sup>. AI presents both significant opportunities and risks. While it enhances threat detection, prediction, and response capabilities, it also introduces new challenges. In total, 56% of leaders believe that generative AI will favour cyber attackers over defenders in the next two years<sup>71</sup>. Leading technological research and consulting firm, Gartner, also placed concerns about AI-enhanced malicious attacks at the top of its emerging risk rankings for Q2 2024<sup>72</sup>.



### The UK National Cyber Security Centre's CEO, Lindy Cameron said:

"We must ensure that we both harness AI technology for its vast potential and manage its risks - including its implications on the cyber threat.

"The emergent use of AI in cyber attacks is evolutionary not revolutionary, meaning that it enhances existing threats like ransomware but does not transform the risk landscape in the near term."

Source: *Global ransomware threat expected to rise with AI, NCSC warns*

AI is not necessarily bringing new risks to the cyber landscape, but it is amplifying the threats that currently exist. For instance, AI lowers the skills required for complex campaigns. Generative AI can help write phishing emails and create custom malware, making it easier for cybercriminals to execute convincing campaigns<sup>73</sup>. In January 2024, scammers exploited deepfake technology to create a group video call, tricking employees of a multinational firm into transferring HK\$200 million<sup>74</sup>. Additionally, advanced cybercriminals and state-backed actors with more funds will have the capacity to develop cutting-edge generative AI hacking tools and share them with the wider hacking community, further increasing attack capabilities of lower-level actors<sup>75</sup>.

By leveraging AI, organisations can enhance their cybersecurity posture, making it easier to detect, predict, and respond to threats in real-time. These models can aid cybersecurity professionals by linking external threats, sensitive data, and unusual activities, thereby identifying risks before they crystallise<sup>76</sup>. Additionally, AI can help address vulnerabilities in the cyber realm, such as human error, which 74% of CISOs identify as their organisation's primary cyber vulnerability<sup>77</sup>. Indeed, more companies are seeking to implement AI tools to guard against cyberattacks that exploit human mistakes<sup>78</sup>. Therefore, investors should ensure that companies leverage AI responsibly, incorporating advanced threat detection tools, real-time incident response mechanisms, and continuous monitoring to mitigate these risks. Robust governance, regular security audits, and compliance with relevant cybersecurity standards are essential to safeguard against the evolving threats posed by AI.


Figure 6: AI trends in cybersecurity

## Opportunities presented by AI




**Increase the efficiency of incident response processes**

Responding to cyber incidents can take days, even weeks, or months. AI can and will continue to speed up the response to these attacks.



**Help security leaders make data-driven decisions**

AI enhances the decision-making process by converting raw data into actionable intelligence, bolstering security strategies and fostering a safer environment.



**Detect and prevent user risk**

AI can be used to analyse users' historical data and interactions to automate safeguards and responses to high-risk users.



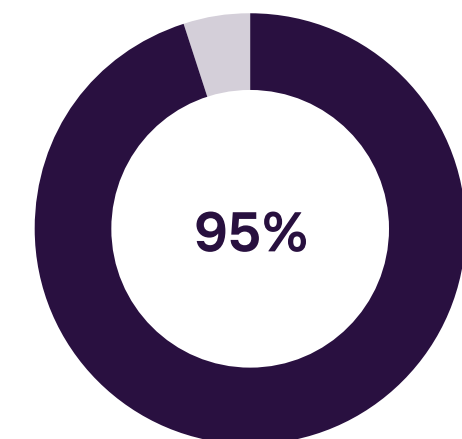
**Augment security nudges & access control policies**

By using AI-powered insights, organisations can strategically and automatically time notifications to match users' online activities. This ensures that security alerts and educational nudges are delivered at the most relevant moments.



**Detect security threats automatically**

AI can automatically detect cybersecurity threats in real time and around the clock, increasing detection rates upwards of...



Source: *Elevate Security (2024), AI in Cybersecurity: Future Trends for 2024*



### 3. Skills shortages

Just as AI is decreasing the skills required to undertake elaborate cyberattacks, the cybersecurity industry is facing a skills shortage. In total, 57% of respondents from the 2023 ISC2 Cybersecurity Workforce Study believe that the shortage of cybersecurity staff is putting organisations in a moderate to extreme risk of experiencing a cybersecurity attack<sup>79</sup>. Despite 464,000 people joining the cybersecurity profession between 2022 and 2023, the shortage of cybersecurity talent continues to deepen, resulting in a global cybersecurity workforce gap of about 3.4 million<sup>80</sup>. The main cause of the cybersecurity skills shortage is the rapid pace at which this landscape is evolving, which is overtaking the speed at which companies can scale their training and hire new workforce<sup>81</sup>.

Two-thirds of organisations face heightened risk because of cybersecurity skills shortages, yet only 15% of firms expect cyber skills to significantly ramp up by 2026<sup>82</sup>. Smaller and public organisations are suffering from this the most as they often lack the budget and capacity to recruit external cybersecurity professionals and compete with salaries offered by larger or private organisations. In the UK, 43% of small and medium-sized enterprises haven't been able to recruit candidates to fill cybersecurity roles<sup>83</sup>.

While acknowledging the aforementioned figures, it is noted that the job market for cybersecurity-related roles reduced by 32% between 2022 and 2023 in the UK<sup>84</sup>. So, rather than there being a lack of skilled people to fill these roles, the gap

could also be due to organisations failing to prioritise cybersecurity risks by increasing their cybersecurity resource budgets and making more roles available.

### 4. Geopolitics

Nation-state and geopolitical cyber threats remain prevalent in the cybersecurity landscape, with 70% of leaders stating that geopolitics has at least moderately influenced their organisation's cybersecurity strategy<sup>85</sup>. Increasing tensions between nations leading to cyber warfare, espionage and critical infrastructure attacks are on the rise. State-sponsored advanced persistent threat (APT) groups are conducting sophisticated and prolonged attacks to steal sensitive data or disrupt operations, and this can often remain undetected for extended periods.

Cyberattacks can serve as both a tool for espionage as well as a weapon for disruption. These attacks have become increasingly widespread since the Russian invasion of Ukraine. Out of 3,662 hacktivist incidents in the EU in the past year, nearly all were linked with the ongoing geopolitical crisis between Russia and Ukraine<sup>86</sup>. For example, a cyberattack on the US satellite communications company, Viasat, in 2022 occurred about an hour before Russia escalated its invasion of Ukraine<sup>87</sup>. This attack disrupted communications for the Ukrainian military, which depended on the satellite, highlighting the strategic use of cyberattacks in modern warfare<sup>88</sup>.





# WHAT SHOULD INVESTORS EXPECT OF PORTFOLIO COMPANIES?

## The Coalition's expectations of companies

As stewards of members' savings and clients' investments, investors have a fiduciary duty to safeguard their portfolios against a myriad of risks, including those posed by cyber threats.

Recognising the importance of this issue and our experience engaging on the topic of cybersecurity, Royal London Asset Management, Railpen and other asset owners have developed a comprehensive set of expectations for investors to use when engaging with portfolio companies on cybersecurity. These expectations are designed to ensure that all stakeholders are aligned in their efforts on cyber risk management.



RAILPEN

### The asset owner's perspective:

Railpen follows the evidence that certain ESG factors, such as cybersecurity, affect the value of the companies we invest in. We believe that by understanding, monitoring and influencing the behaviour of those companies, we can help ensure our portfolios are resilient to material ESG risks and, as a result, protect and enhance the long-term value of members' savings.

While Railpen is unusual amongst UK asset owners in managing most of its assets in-house, we appreciate the importance of an aligned approach with our external managers. We are responsible for ensuring that external managers' stewardship and sustainable investment policies align with the Trustee's own policies.

Therefore, recognising the importance of cybersecurity resilience, we would encourage asset managers to develop their understanding of the financial materiality of cybersecurity, use the investor expectations as a tool for engagement with companies that face a high level of risk, and report on progress to their clients.



### The asset manager's perspective:

Royal London Asset Management believes that driving corporate change requires a collaborative effort from asset managers, asset owners, regulators and policy makers. The Coalition was established following calls to action from Nest and Railpen to fund managers, like Royal London Asset Management, to enhance and develop frameworks to help address potential cybersecurity risks to client portfolios. We initiated this collaborative effort to help asset owners tackle this issue and to broaden our shared knowledge and expertise.

Acting as the secretariat of this Coalition, our responsibilities included the co-creation of a methodology to evaluate corporate behaviour, identifying underperforming companies through data analysis, organising meetings, and sharing best practices. Initially, the programme focused on engagement for information, as cybersecurity disclosures were limited. We understood the importance of collaborative engagement and dialogue with companies to enhance transparency regarding cybersecurity processes, given the potential business risks. Through these interactions, we identified best practices that guided the formulation of the investor expectations outlined in this report.

We encourage asset managers to adopt our investor expectations to enhance the management of cyber risks within their portfolios.





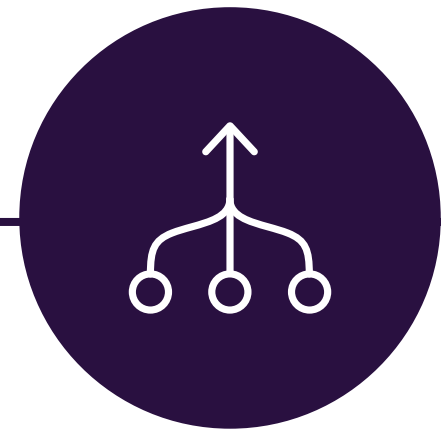
## Our four pillars

In this section of the report, we explain what our expectations are across each of our four pillars, why each expectation is important and how to implement them. In addition, we have included anonymised case studies to demonstrate best practices exhibited by companies the Cybersecurity Coalition has engaged with.



### Governance

Robust board oversight is essential for implementing effective cybersecurity practices. Ensuring that the board is actively involved in cybersecurity governance helps in setting the right tone at the top and aligning cybersecurity strategies with business objectives.



### Supply chain and mergers & acquisitions (M&A)

Comprehensive due diligence and proactive risk management of external parties are critical. This includes assessing the cybersecurity posture of suppliers and acquisition targets to mitigate risks and ensure the integrity of the supply chain.



### Processes, culture and training

Fostering a resilient culture is fundamental and should be supported by strong vulnerability management and penetration testing; obtaining relevant cybersecurity certifications ensures that daily operations are secure and reduces the risk of cyber incidents.



### Collaboration

Working with peers and government bodies is crucial to enhancing cybersecurity standards. Collaborative efforts can lead to the sharing of best practices, threat intelligence, and coordinated responses to cyber threats.



Pillar	Investor expectation
<b>Governance</b>	<ul style="list-style-type: none"> <li>• A nominated CISO, or equivalent, with supporting resources</li> <li>• Risk identification and oversight at board level</li> <li>• Timely disclosure of cybersecurity breaches</li> <li>• Inclusion of information security and cyber resilience in executive compensation key performance indicators (KPIs)</li> <li>• Evaluation of cybersecurity in board effectiveness reviews</li> </ul>
<b>Supply chain/M&amp;A</b>	<ul style="list-style-type: none"> <li>• Effective due diligence and monitoring of supply chain cybersecurity, in addition to including cyber covenants in supplier contracts</li> <li>• Inclusion of cyber considerations in inorganic growth strategies, including in the due diligence and integration phases</li> </ul>
<b>Processes, culture and training</b>	<ul style="list-style-type: none"> <li>• Disclosures about a cyber-resilient culture should include innovative and tailored training programs across the workforce</li> <li>• Vulnerability management and penetration testing, such as the use of ethical hacking</li> <li>• Relevant cyber certification maintained, or independent audit report held</li> </ul>
<b>Collaboration</b>	<ul style="list-style-type: none"> <li>• Collaboration with peers and government bodies to raise cybersecurity standards and manage systemic risk</li> </ul>

## Governance

### A nominated CISO, or equivalent, with supporting resources

Having a CISO, or equivalent, with the appropriate resources and buy-in from senior leadership is essential for effectively managing a company's cybersecurity landscape. The CISO provides dedicated leadership and strategic direction, ensuring that cybersecurity measures are robust, up-to-date, and align with the company's overall risk-management framework. By overseeing the implementation and monitoring of security protocols, the CISO helps mitigate potential cyber threats and vulnerabilities.

Investors should expect a clear governance structure around cybersecurity risk, featuring well-defined responsibilities, dedicated teams, and clear lines of accountability. Public disclosures should highlight the presence of a CISO, or equivalent, and detail how they are supported by a specialised team. This approach ensures that cybersecurity strategies are consistently implemented, monitored across the company, and reported to the board.

### Risk identification and oversight at board level

Identifying and overseeing cyber risk at board level is critical. Board-level oversight ensures that cybersecurity is prioritised and integrated into the broader risk-management framework, enabling proactive measures to mitigate potential threats. Additionally, having the board involved in cybersecurity governance fosters a culture

of accountability and transparency. Ultimately, effective board oversight of cyber risk enhances an organisation's resilience and ability to respond swiftly and effectively to cyber incidents.

Investors should expect that the cybersecurity technical team, or the CISO, regularly reports to the board, ensuring members remain well-informed about the organisation's cyber risk landscape. Best practice includes a dedicated board committee or board member responsible for cybersecurity oversight. To effectively fulfil this role, the board must possess sufficient cybersecurity expertise. This can be achieved by having board members with cybersecurity skills, engaging independent cybersecurity advisors, or implementing a comprehensive training program for board members. A comprehensive training program will cover day-to-day oversight, alongside practical desktop exercises to simulate a real-time cybersecurity breach and appropriate response mechanisms. Given the evolving landscape, training should not be considered a 'once and done' exercise.

In a recent article by Nili and Shapira, it is recognised that the appointment of 'specialist directors' may have unforeseen consequences on corporate behaviour, including the creation of an authority bias and overly increasing the size of boards<sup>89</sup>. Therefore, we consider previous experience, upskilling and external advisory services to be equally relevant.





## Timely disclosure of cybersecurity breaches

In December 2023, the SEC issued a new ruling mandating listed companies to report annually their processes for monitoring and managing cyber threats. The rules require the disclosure of cybersecurity risks and breaches in their public filings within four days of identifying a 'material' cybersecurity incident. However, this does not apply to other jurisdictions.

Timely disclosure of significant breaches is crucial for maintaining trust and transparency between a company and its stakeholders. Best practices include disclosing how significant cyber threats are managed. Companies are expected to publicly disclose any significant breaches through company reporting or, if outside the reporting cycle, via a dedicated press release or webpage. Investors should expect prompt communication that demonstrates the company is taking necessary precautions and shows a commitment to security and accountability. Investors should encourage companies to disclose lessons learned and remedial actions taken post-breach.

## Inclusion of information security and cyber resilience in executive compensation KPIs

This aligns executive incentives with the company's long-term security goals, ensuring that top management prioritises robust cybersecurity measures. For investors, this is crucial as it demonstrates a company's commitment to proactively managing cyber risks. By tying executive compensation to cybersecurity performance, investors can be more confident that the company is taking comprehensive steps to safeguard its assets and reputation against cyber threats.

## Evaluation of cybersecurity in board effectiveness reviews

This is vital for investors as it ensures that boards possess the necessary expertise to oversee and mitigate cyber risks. This evaluation provides investors with confidence that the board can effectively navigate the complexities of cybersecurity, implement robust protective measures, and respond swiftly to incidents. It also indicates that the company prioritises cybersecurity at the highest level of governance, aligning with best practices and regulatory expectations.

Investors should encourage company boards to evaluate cybersecurity skills as part of a board effectiveness review. This review should be transparent, with clear disclosure of the findings and any actions taken if the board doesn't meet the necessary requirements.

## Supply chain and mergers & acquisitions (M&A)

### Effective due diligence and monitoring of supply chain cybersecurity, in addition to including cyber covenants in supplier contracts

Supply chain cyber risk management is crucial to investors because it directly impacts a company's operational resilience. In today's interconnected business environment, a cyber incident affecting a supplier can quickly cascade, disrupting operations, compromising sensitive data, and potentially cause financial losses. Effective supply chain cyber risk management ensures that a company has robust measures in place to identify, assess, and mitigate these risks, thereby safeguarding its operations.

Investors should expect a comprehensive approach to effective due diligence and monitoring of supply chain cybersecurity. This approach could include provisions such as an annual right to audit within supplier contracts or a clear code of conduct for suppliers with conditions related to cybersecurity management.



### What good looks like: Supply chain monitoring

A global oil and gas company provides detailed reporting on the management of suppliers in relation to cybersecurity. One of the top five cyber risks to the business is disruption to operations, which can originate from either the company or third-party sources. The company recognises the importance of considering not only its own digital infrastructure but also the services provided by other companies, including non-technology firms.

The company has implemented a specific programme for supplier security, where new suppliers undergo a rigorous process that includes both external and internal intelligence, as well as third-party security rankings. This information is used to assess the supplier's risk based on the nature of their work, their reach, and breadth of activities. The company also evaluates the supplier's visibility of their systems and their risk assessment. In addition to information security requirements, standard clauses are included in supplier contracts, with some requiring negotiation. Once a supplier is selected, a standard set of cyber risk clauses is embedded into contracts. Suppliers are tiered and factored into the risk assessment, and while not all suppliers include the covenant to the right to audit, this is negotiated with each supplier.



## Inclusion of cyber considerations in inorganic growth strategies including in the due diligence and integration phases

Failing to complete effective due diligence and integration of cyber considerations in M&A can expose companies to significant risks. Without thorough cyber due diligence, the acquiring company may inherit vulnerabilities from the target company. Cyber incidents post-acquisition can disrupt business operations and erode shareholder value<sup>90</sup>. In some cases, these risks can even jeopardise the success of the deal itself, as seen in past high-profile M&A transactions where cyber issues led to reduced purchase prices or deal cancellations<sup>91</sup>. Therefore, integrating robust cyber considerations into the M&A process is essential to safeguard the investment and ensure long-term stability.

Investors should engage with companies to provide clear evidence and disclosure of how cyber considerations are integrated into inorganic growth strategies, encompassing both the due diligence and integration phases. This may include requests for penetration test results, outcomes from red teaming exercises<sup>d</sup>, and other relevant cybersecurity assessments.

<sup>d</sup> A red team is a group of security professionals who simulate attacks on an organisation's systems to identify vulnerabilities and improve defences.

## Processes, culture & training

### Disclosures about a cyber-resilient culture, to include innovative and tailored training across the workforce

Investors should request evidence and disclosure of engaging and innovative cybersecurity training programmes, such as simulations and gamified workforce training. Additionally, companies should provide public disclosures on their cyber-resilient culture and offer tailored and regularly updated training for specific roles, including the leadership team. These measures demonstrate a commitment to fostering a robust cybersecurity environment and ensuring that all employees, particularly those in critical positions, are well-prepared to address cyber threats.



#### What good looks like: Improved data-protection training

A major UK airport faced a cybersecurity incident that highlighted the need for improved data-protection training. In response, the airport implemented comprehensive training programmes for all employees, including mandatory cybersecurity training and specialised sessions for privileged users, as required by the Aviation Security Act. Regular phishing tests and targeted education were introduced to raise awareness, along with training on social engineering tactics. New recruits, especially those in physical security roles, receive tailored cybersecurity training to ensure they are well-prepared.



## Vulnerability management and penetration testing, such as the use of ethical hacking

Investors should engage with companies to understand whether they have a comprehensive vulnerability management programme which entails the timely identification, management, and remediation of vulnerabilities, complemented by regular penetration testing. If there are specific findings from the testing, investors should encourage companies to disclose their learnings and any remediation efforts. Investors should also request information on the types of testing conducted and their frequency.

## Relevant cyber certification maintained, or independent audit report held

Maintaining a relevant cyber certification or holding an independent audit report is crucial for investors as it demonstrates a company's commitment to robust cybersecurity practices and regulatory compliance. For the purposes of best practice, investors should request that companies reference their certifications and frameworks in public disclosures. Once disclosed, investors should also pay attention to the certifications' level of coverage across a company's operations as this may reveal a vulnerability in its digital estate.

Investors should encourage companies to hold certifications such as ISO27001<sup>92</sup> or Cyber Essentials+<sup>93</sup> for all operations, or alternatively, follow the NIST framework<sup>94</sup> or an equivalent standard. Furthermore, holding an external audit report like SOC 2 Type 2<sup>95</sup> or ISAE3402<sup>96</sup> for all operations provides an added layer of assurance. These certifications and audits provide assurance that the company has implemented effective measures to protect sensitive data and mitigate cyber risks.



### What good looks like: Cybersecurity certification

An international bank exemplifies industry best practices in cyber risk management. The CISO emphasised that their risk policies are aligned with NIST and ISO 27001 standards, ensuring adherence to recognised best practices.

The bank's first line of defence is an internal control testing team, which is incentivised to identify issues, with 68% of issues being self-discovered. Additionally, external audits conducted by an independent third party cover all operations and internal controls.

The bank has implemented a comprehensive approach to vulnerability management. This includes conducting penetration testing for even minor code changes, maintaining a 15-person strong red team, and performing regular vulnerability scanning. Leveraging significant industry experience, the CISO estimated that the organisation has the lowest level of vulnerability per asset in the industry. The organisation benchmarks itself against peers, with another global bank serving as the closest comparator, and also benchmarks geographically against local banks.

## Collaboration

### Collaboration with peers and government bodies to raise cybersecurity standards and manage systemic risk

This is essential for companies because it strengthens their overall security posture and resilience against cyber threats. By engaging in cooperative efforts, companies can benefit from shared knowledge, resources, and best practices, which enhances their ability to detect, prevent, and respond to cyber incidents.

This collective approach helps mitigate systemic risks that could disrupt business operations and lead to significant financial and reputational damage. Furthermore, aligning with regulatory requirements and industry standards through collaboration ensures compliance and reduces the risk of legal penalties.

Investors should encourage companies to take a leadership role in driving cybersecurity standards and managing risks through collaboration with peers and government bodies. Additionally, companies should publicly disclose their collaborative efforts in cybersecurity, providing evidence of the outcomes achieved.



## WHAT CAN INVESTORS DO?

There are a number of actions investors can take to tackle the increasing cybersecurity risks faced by portfolio companies.



**1** As a first and critical step, we invite investors to **recognise cybersecurity as a financially material ESG risk**, which is supported by the evidence provided in this report.



**2** We encourage investors to **use the expectations outlined in this report** to assess companies' baseline approach to cybersecurity and to measure companies' progress towards best practice.



**3** It's important to **identify and engage with companies that face high-risk exposure**, using sector-specific vulnerabilities as a lens for screening and our recommended questions to initiate dialogue. As stewards of members' savings, with a responsibility to monitor external managers' approaches, asset owners should encourage asset managers to engage with portfolio companies on their cybersecurity resilience. This can begin with stewardship dialogue and, if progress is lagging or insufficient, we suggest escalation.



**4** We recommend **participation in policy advocacy on cybersecurity**. A supportive regulatory environment will enable improved alignment between company disclosures and investors' expectations.



## How to put these steps into action

### Identify companies with high sectoral risk exposure

Investors should identify highly-exposed companies, so that resources can be focused on areas where the risk is most material. Looking at exposure through a sectoral lens is one path to achieving this. However, a company's sector must be considered alongside other factors, such as regulatory oversight, size and geography. For example, the Cybersecurity Coalition targeted the energy and utilities sector in its first phase of engagement, but found that the sector was better prepared to face these risks due to the regulatory environment.

Identifying the laggards in vulnerable sectors can enable investors to proactively engage with companies in order to mitigate the likelihood of a cyber incident occurring and increase resilience if the risk does materialise. Although there is debate surrounding which industries are most vulnerable to cyberattacks, the leaders generally include healthcare, manufacturing, finance and insurance, and energy and utilities<sup>e</sup>. The impact of cybersecurity risks materialising in these industries is demonstrated on the next two pages through a series of case studies on companies that have experienced major incidents.

<sup>e</sup> Although public administration is a highly vulnerable sector as well, this report will not focus on it due to the lack of direct exposure of typical institutional investors to this sector.

## Healthcare



In 2023, healthcare organisations experienced the most data breaches since 2009<sup>97</sup>. The 2023 Third-Party Data Breach Report by risk management firm, Black Kite, states that the healthcare industry was the most targeted victim of third-party breaches, accounting for almost 35% of all incidents in 2022<sup>98</sup>.

Healthcare is not only a vulnerable sector in terms of frequency of incidents, but also due to the costs incurred and longer-term impact on customers. Indeed, the healthcare industry has been paying the highest average data breach cost compared to other industries since 2010<sup>99</sup>.

Healthcare organisations are prone to cyberattacks as they possess extensive data that is of substantial economic and strategic worth to cybercriminals and governmental adversaries, such as patients' confidential health details, financial information, personal identification numbers, and insight into medical research and innovation.



### Case study:

#### Cybersecurity event:

On the 2 May 2023, Perry Johnson & Associates (PJ&A), a privately-held US medical transcription services company discovered it had been the victim of a cyberattack. PJ&A was a supplier used by many companies and therefore the attackers targeted sensitive personal data, including social security numbers, insurance information and clinical data.

#### Impact:

In total, 13 million record holders were compromised in this attack, mainly stemming from hospital clients<sup>100</sup>. PJ&A lost 3 of its 8 major clients after the attack and more than 40 class-action lawsuits related to the attack have been filed<sup>101</sup>. A non-profit focused on information risk, The Fair Institute, estimated primary costs from this attack to be US\$4.7 million, with secondary costs reaching US\$8.1 million<sup>102</sup>.

## Manufacturing



The widely recognised 2024 Threat Intelligence Index by IBM states that manufacturing is one of the most attacked industries<sup>103</sup>. The manufacturing sector's vulnerability to cyber threats is attributed to its dependence on interconnected and often outdated systems, which are integral to operational efficiency. These systems are prime targets for data theft, intellectual property infringement, and operational disruption. The convergence of IT and operational technology has expanded the attack surface, while legacy systems lacking in cybersecurity measures compound the vulnerability.

The average cost per breach for the sector went up more than any other industry in 2023, increasing by US\$830,000 compared to the previous year<sup>104</sup>. This higher cost could be due to attempts to react and restore systems quickly, as their operations are very sensitive to downtime<sup>105</sup>. However, the time it took for industrial organisations to find and contain a data breach was longer than the median industry<sup>106</sup>.



### Case study:

#### Cybersecurity event:

In February 2023, the US company, Applied Materials, which provides technology for the semiconductor industry, reported a ransomware attack on one of their suppliers (assumed to be MKS instruments)<sup>107</sup>. MKS filed notice of a data breach after learning of the ransomware attack that resulted in sensitive employee information being made accessible to an unauthorised party.

#### Impact:

The ransomware event had a material impact in the first quarter on the company's ability to process orders, ship products and provide services to customers<sup>108</sup>. This cyberattack was reported to have cost Applied Materials US\$250 million<sup>109</sup>.

With growing geopolitical tensions between the US and China, cyberattacks like this one on the semiconductor manufacturing supply chain may become more prevalent.

## Finance and insurance



### Case study:

#### Cybersecurity event:

The Equifax cyberattack in 2017 exposed the personal information of nearly 143 million Americans<sup>113</sup>. Hackers exploited a vulnerability in Equifax's systems, leading to the theft of sensitive data like social security numbers and addresses.

#### Impact:

Moody's estimated that Equifax's cybersecurity expenditure would reach "US\$400 million in both 2019 and 2020 before declining to about US\$250 million in 2021"<sup>114</sup>. As a result, Equifax was the first company to have its outlook downgraded due to a cybersecurity attack, from Baa1 to Baa2<sup>115</sup>. Additionally, the breach resulted in multiple investigations and fines. For instance, the Financial Conduct Authority (FCA) fined Equifax Ltd £11 million for failing to manage and monitor the security of UK consumer data<sup>116</sup>.

In the past two decades, nearly one-fifth of reported cyber incidents have affected the global financial sector, causing US\$12 billion in direct losses to financial firms<sup>110</sup>. The IBM 2023 Cost of a Data Breach report states that the finance and insurance industry has the second highest average cost per breach<sup>111</sup>.

The increasing number of attacks, combined with high costs, means that this sector should not be overlooked. Its vulnerability can be explained through the large amounts of customer data and transactions handled, alongside its systemic implications for economic activity. The IMF identifies three characteristics that further increase the vulnerability of financial institutions to cyber incidents: market concentration, dependence on third-party IT providers, and interconnectedness among financial institutions<sup>112</sup>.



## Energy and utilities



The energy and utilities sector is among the top five most targeted industries overall<sup>117</sup>. Almost 60% of cyberattacks against energy and utility companies are led by nation-state affiliated groups<sup>118</sup>. MI5, MI6, the National Cyber Security Centre and the National Crime Agency have issued warnings on potential cyber threats to UK infrastructure, including on the UK's electricity and gas networks<sup>119</sup>.

As cyberattacks can jeopardise the security of energy supply and the privacy of consumer data, it is a prime target for cyber attackers. Additionally, the increasing digitalisation and connectivity of this sector creates new risks, due to an expanded attack surface<sup>120</sup>.



### Case study:

#### Cybersecurity event:

In May 2021, the Colonial Pipeline, the largest fuel pipeline in the United States, was targeted by the DarkSide ransomware group<sup>121</sup>.

#### Impact:

The attackers gained access through a compromised VPN account, encrypting the company's data and demanding a US\$4.4 million ransom<sup>122</sup>. The company decided to pay the ransom and operations had to shut down, leading to significant fuel shortages<sup>123</sup>.



## Engage with target companies

### Stewardship dialogue

We recognise that the key to effective cybersecurity risk management is a company's preparedness for an incident and ability to recover from both outages and ransomware-style attacks in a timely manner. Therefore, investors should engage with highly-exposed companies to understand their approach. Where asset owners appoint asset managers to lead engagement with portfolio companies, we advise them to encourage a greater focus on this topic.

To assess a company's resilience, we recommend that investors consider asking the following questions...



#### Governance

- Is your organisation's approach and policy on cybersecurity overseen and managed at board level?
- Are there regular board discussions on cybersecurity, based on timely and accurate information that's informed by expert guidance?
- Do the cybersecurity KPIs being reported to your board capture the extent of the current security weaknesses across your digital estate to ensure the risk is truly understood?
- Is a member of the board accountable for cybersecurity and does the board engage in regular discussions on the issue?
- Have all necessary roles and responsibilities related to cybersecurity been clearly identified?



#### Supply chain and mergers & acquisitions (M&A)

- How does your organisation monitor and conduct due diligence on your supply chain in relation to cybersecurity?
- How does your organisation monitor and protect its information perimeter across the group and globally?
- How are cybersecurity considerations included in M&A activity, particularly during the due diligence and integration phases?



#### Processes, culture and training

- To which industry-recognised frameworks are your processes aligned in relation to cyber risks?
- What activities (such as vulnerability scanning, penetration testing and auditing) are undertaken to provide assurance that your organisation's security controls are effective?
- Are your critical services, products and data subject to immutable backups, to ensure integrity and recovery from ransomware-style incidents?
- Do you have business continuity and disaster recovery plans in place to ensure the continuation of services in the event of a cyber incident on your organisation? Do you test the effectiveness of these plans? Does this include ensuring recoverability from ransomware incidents and service resilience to outages?
- How does your organisation ensure that there is a cyber-resilient culture across the group?
- What cybersecurity training programme does your organisation have in place, and how is it tailored to key individuals or teams?



#### Collaboration

- How does your organisation collaborate with government bodies and peers to raise cybersecurity standards and manage systemic risk?
- What specific initiatives or programmes has your organisation joined/implemented to enhance collaboration in cybersecurity?
- How does your organisation stay updated on the latest cybersecurity threats and trends through collaboration with external entities?



“It has been a privilege to support our Sustainable Ownership team in their engagement with portfolio companies. I’d encourage others to include their relevant subject-matter experts as part of their own pre-investment and ongoing due diligence processes. Effective cybersecurity management is crucial for protecting assets, thereby maintaining investor trust and long-term shareholder value. It’s a collective responsibility that involves the entire organisation, requiring oversight and sponsorship at the highest levels. When cybersecurity issues arise, they can cause financial and reputational risks for companies that may impact their performance. Effective governance and risk management practices can be the difference between responding to a defensible or indefensible position.”

**Shaun Roberts, Railpen CISO**

### Use of subject-matter experts

We recommend that investors, where feasible, invite subject-matter experts to participate in engagement calls with portfolio companies. Within the Cybersecurity Coalition’s engagement programme, these experts have reviewed our investor expectations to ensure alignment with market best practice. During engagement, they have provided technical perspectives on potential concerns for investors and identified areas requiring further dialogue. This approach assists stewardship teams in setting clear objectives for engagement and supports investment teams in monitoring investee companies.

### Escalation

Where a company fails to respond to questions on cybersecurity or is deemed to fall far below investor expectations on best practice, escalation can be a useful tool to secure a response or encourage change (see Figure 7). Within the Coalition, Railpen and Royal London Asset Management have sought to engage with companies in a confidential and constructive manner without publicity as we expect good management to reassure investors when faced with shareholders’ concerns. However, we reserve the right to make our concerns public if the company fails to adequately address the issues that have been raised. An example of this process being put into practice can be found to the right in our case study.

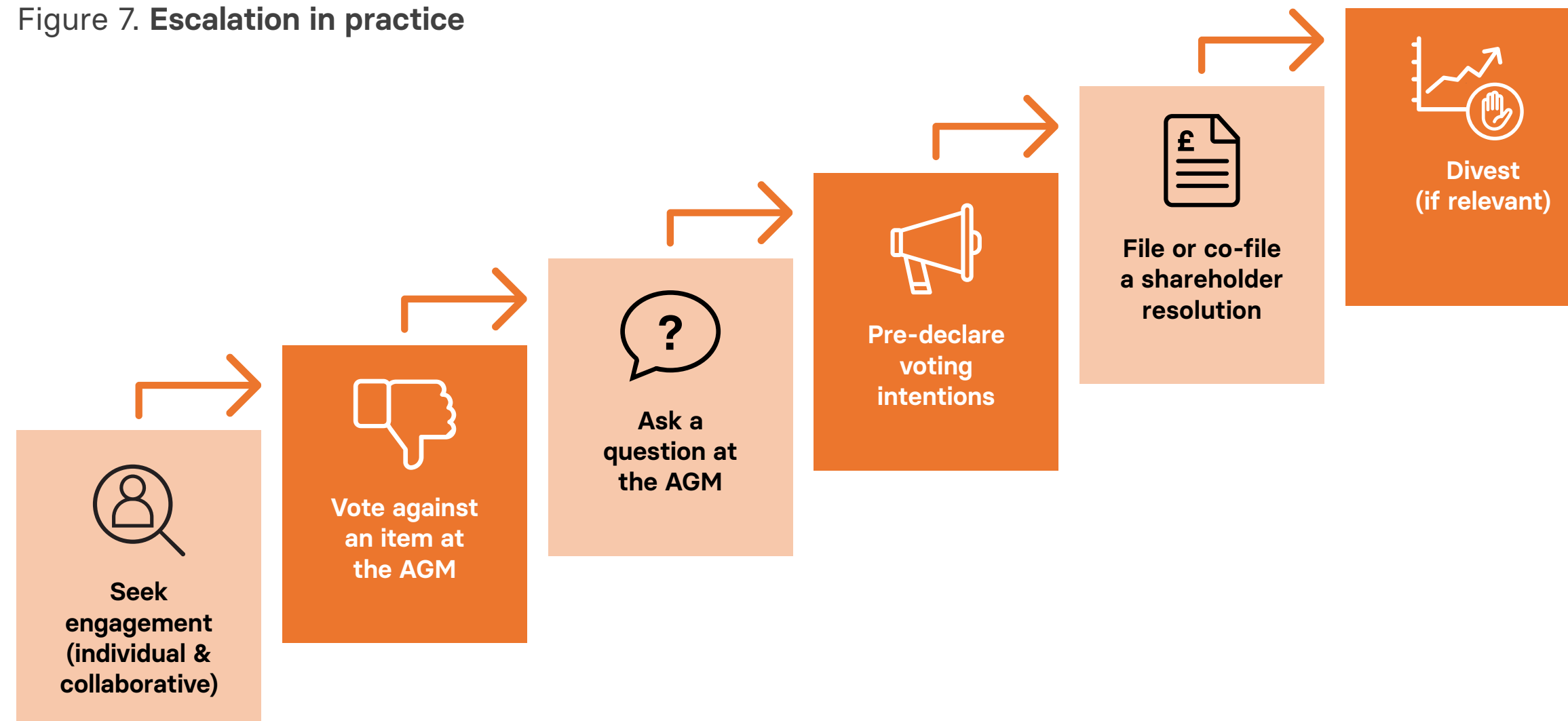
### Case study: Escalation

A pharmaceutical company was selected for engagement by Railpen due to its growing digital footprint and failure to meet the Cybersecurity Coalition’s expectations on disclosure. The company was initially unresponsive, so we signalled our concerns by voting against the director we deemed to be responsible for risk oversight – the Chair of the Audit Committee. We also asked a question at the 2022 AGM on the materiality of cybersecurity and repeated our request for a meeting.

Following this escalation, we were able to establish dialogue with subject-matter experts at the company. During discussions, we encouraged them to align their reporting with our investor expectations. Post-engagement, we were pleased to see that director biographies had been updated to include additional skills of interest to shareholders, such as cybersecurity experience. There is also now a dedicated section on cybersecurity within the company’s ESG report, which provides reassurance on risk controls and oversight through disclosure of the following:

- The Audit Committee’s oversight role
- The presence of a CISO
- Tailored cyber training across the workforce
- Monitoring of suppliers’ approach to cybersecurity procedures.

Figure 7. Escalation in practice





## Participate in policy advocacy

System-wide issues, like cybersecurity, require system-wide responses. Investors should actively engage in public policy advocacy regarding cybersecurity, including responding to consultations such as those from the SEC on cyber reporting. By undertaking public policy advocacy, investors can help shape the regulatory landscape to support positive cybersecurity outcomes and ensure that the standards set by bodies like the SEC are practical, effective, and aligned with the realities of the market. This proactive involvement can lead to regulations that better protect both investors and companies.

Railpen and Royal London Asset Management incorporate proactive and reactive advocacy into their stewardship programmes. On cybersecurity specifically we have, for instance, responded to the SEC consultation on Proposed Rule S7-09-22<sup>f</sup>.

<sup>f</sup> Railpen's response to the SEC's Proposed Rule S7-09-22 is available at [cdn-suk-railpencom-live-001.azureedge.net/media/media/apvelsud/sec-proposed-rule-submission\\_final-060522.pdf](https://cdn-suk-railpencom-live-001.azureedge.net/media/media/apvelsud/sec-proposed-rule-submission_final-060522.pdf)

RLAM's response is available at [rlam.com/uk/institutional-investors/our-views/2023/sec-new-cyber-security-expectations/](https://rlam.com/uk/institutional-investors/our-views/2023/sec-new-cyber-security-expectations/)

Policy advocacy on cybersecurity can be put into the following categories:

- 1 Focus on strong cybersecurity practices:** Effective cybersecurity is crucial for the long-term success of companies. By advocating for robust cybersecurity practices, investors can help reduce material risks of cyber incidents that could negatively impact their portfolios.
- 2 Call for greater transparency on cybersecurity disclosure:** Greater transparency in how companies manage cybersecurity risks can allow investors to make more informed decisions and hold companies to account. This approach enhances investors' oversight, ensuring that we continue to be responsible stewards of our member's savings and clients' money.

Investors' incorporation of public policy advocacy into their system-wide stewardship work is still in its infancy. Railpen has worked with the ICGN on its Systemic Stewardship & Public Policy Advocacy Toolkit<sup>124</sup>, in which investors considering advocacy are given the following guidance:

- Assess both the need for advocacy and available resources
- Create a strategy
- Develop the public policy approach
- Implement the plan
- Track progress
- Report on it.

When putting this into practice, we encourage stewardship practitioners to collaborate closely with their relevant specialist teams.

For more information visit: [ICGN Systemic Stewardship & Public Policy Advocacy Toolkit September 2023](#)



# REFERENCES

- 1 WEF (2024), Global Cybersecurity Outlook 2024, [WEF Global Cybersecurity Outlook 2024.pdf \(weforum.org\)](#)
- 2 IBM (2024), Cost of a Data Breach Report 2024, [Cost of a Data Breach Report 2024 \(ibm.com\)](#)
- 3 IMF (2024), Global Financial Stability Report, [The Last Mile: Financial Vulnerabilities and Risks \(imf.org\)](#)
- 4 WEF (2024), Global Cybersecurity Outlook 2024, [WEF Global Cybersecurity Outlook 2024.pdf \(weforum.org\)](#)
- 5 IMF (2024), Global Financial Stability Report, [The Last Mile: Financial Vulnerabilities and Risks \(imf.org\)](#)
- 6 Mimecast (2024), The State of Email & Collaboration Security Report 2024, [Mimecast-State-of-email-and-collaboration-security-Report-2024](#)
- 7 Keeper (2022), 2022 US Cybersecurity Census Report, [2022-US-Cybersecurity-Census.pdf \(keeper.io\)](#)
- 8 UK Government Department for Science, Innovation & Technology (2024), Cyber security breaches survey 2024, [Cyber security breaches survey 2024 - GOV.UK \(www.gov.uk\)](#)
- 9 Proofpoint (2024), 2024 Voice of the CISO, [2024 Voice of the CISO \(nationalcioreview.com\)](#)
- 10 Ibid
- 11 Ponemon Institute and Optiv (2024), 2024 Cybersecurity Threat and Risk Management Report, [2024 Cybersecurity Threat and Risk Management Report | Optiv](#)
- 12 Moody's (2023), 2023 Cyber Survey Highlights, [Moody's Cyber Survey \(moodys.com\)](#)
- 13 National Institute of Standards and Technology (2024), Glossary: Cybersecurity Incident, [Cybersecurity Incident - Glossary | CSRC \(nist.gov\)](#)
- 14 IBM (2024), Cost of a Data Breach Report 2024, [Cost of a Data Breach Report 2024 \(ibm.com\)](#)
- 15 European Union Agency for Cybersecurity (2024), ENISA Threat Landscape 2024, [ENISA Threat Landscape 2024 — ENISA \(europa.eu\)](#)
- 16 NIST (2022), Ransomware Risk Management: A Cybersecurity Framework Profile (NISTIR 8374), [Final Ransomware Risk Management CSF Profile & Quick Start Guide Released | CSRC \(nist.gov\)](#)
- 17 Akamai (2023), Defeating Triple Extortion Ransomware: The Potent Combo of Ransomware and DDoS Attacks, [Defeating Triple Extortion Ransomware: The Potent Combo of Ransomware and DDoS Attacks | Akamai](#)
- 18 IBM (2024), Cost of a Data Breach Report 2024, [Cost of a Data Breach Report 2024 \(ibm.com\)](#)
- 19 Ibid
- 20 FAIR Institute (2020), Primary vs. Secondary Loss in FAIR™ Analysis: What's the Difference and Why It Matters, [Primary vs. Secondary Loss in FAIR™ Analysis: What's the Difference and Why It Matters \(fairinstitute.org\)](#)
- 21 Moody's Analytics (2023), The impact of cyber security management practices on the likelihood of cyber events and its effect on financial risk, [the-impact-of-cyber-security-management-practices.pdf \(moodys.com\)](#)
- 22 UK National Cyber Security Centre and National Crime Agency (2024), Ransomware, extortion and the cyber crime ecosystem, [Ransomware, extortion and the cyber crime ecosystem \(ncsc.gov.uk\)](#)
- 23 Sophos (2024), The State of Ransomware 2024, [sophos-state-of-ransomware-2024-wp.pdf](#)
- 24 Ibid
- 25 Ibid
- 26 Ibid
- 27 Ibid
- 28 Ibid; Howden (2024), Cyber Insurance: Risk, Resilience and Relevance, [howden-2024-cyber-report.pdf \(howdengroupholdings.com\)](#)
- 29 Ibid
- 30 Enterprise Management Associates (2024), IT outages: 2024 costs and containment, [EMA-BigPanda-final-Outage-eBook.pdf](#)
- 31 IBM (2024), Cost of a Data Breach Report 2024, [Cost of a Data Breach Report 2024 \(ibm.com\)](#)
- 32 Howden (2024), Cyber Insurance: Risk, Resilience and Relevance, [howden-2024-cyber-report.pdf \(howdengroupholdings.com\)](#)
- 33 Moody's (2023), 2023 Cyber Survey Highlights, [Moody's Cyber Survey \(moodys.com\)](#)
- 34 The Ponemon Institute and Optiv (2024), 2024 Cybersecurity Threat and Risk Management Report, [2024-Cybersecurity-Threat-and-Risk Management-Report.pdf \(optiv.com\)](#)
- 35 Ibid
- 36 Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019), 'Content analysis of cyber insurance policies: how do carriers price cyber risk?' *Journal of Cybersecurity*, 5(1), <https://doi.org/10.1093/cybsec/tyz002>
- 37 Ibid; Howden (2024), Cyber Insurance: Risk, Resilience and Relevance, [howden-2024-cyber-report.pdf \(howdengroupholdings.com\)](#)
- 38 Howden (2024), Cyber Insurance: Risk, Resilience and Relevance, [howden-2024-cyber-report.pdf \(howdengroupholdings.com\)](#)
- 39 Comparitech (2024), How data breaches affect stock market share prices, [How data breaches affect stock market share prices - Comparitech](#)
- 40 Moody's Analytics (2023), The impact of cyber security management practices on the likelihood of cyber events and its effect on financial risk, [the-impact-of-cyber-security-management-practices.pdf \(moodys.com\)](#)
- 41 IMF (2024), Global Financial Stability Report, [The Last Mile: Financial Vulnerabilities and Risks \(imf.org\)](#)
- 42 Harvard Business Review (2020), A Cyberattack Doesn't Have to Sink Your Stock Price, [A Cyberattack Doesn't Have to Sink Your Stock Price \(hbr.org\)](#)
- 43 The Ponemon Institute and Centrify (2017), How Data Breaches Affect Reputation & Share Value: A Study of U.S. Marketers, IT Practitioners and Consumers, [How data breaches affect reputation and share value | Ponemon-Sullivan Privacy Report \(ponemonsullivanreport.com\)](#)
- 44 Cybersecurity Dive (2024), Cyberattacks pose mounting risks to creditworthiness: Moody's, [Cyberattacks pose mounting risks to creditworthiness: Moody's | Cybersecurity Dive](#)
- 45 Ibid
- 46 Sheneman, A. (2017), 'Cybersecurity Risk and the Cost of Debt', SSRN, <http://dx.doi.org/10.2139/ssrn.3406217>
- 47 Chen, P., S. He, Z. Ma, & D. Stice. (2016), 'The information role of audit opinions in debt contracting' *Journal of Accounting and Economics* 61 (1): 121-144, <https://doi.org/10.1016/j.jacceco.2015.04.002>; Kim, J.B., B.Y. Song, and L. Zhang. (2011), 'Internal control weakness and bank loan contracting: Evidence from SOX Section 404 disclosures' *The Accounting Review* 86 (4): 1157-1188, <https://doi.org/10.2308/accr-10036>
- 48 Rosati, P., Gogolin, F., & Lynn, T. (2019), 'Audit firm assessments of cyber-security risk: evidence from audit fees and SEC comment letters' *The International Journal of Accounting*, 54(03), 1950013, <https://doi.org/10.1142/S1094406019500136>; Rosati, P., Gogolin, F., & Lynn, T. (2022), 'Cyber-security incidents and audit quality' *European Accounting Review*, 31(3), 701-728, <https://doi.org/10.1080/09638180.2020.1856162>
- 49 Ibid
- 50 National Institute of Standards and Technology (2024), Glossary: Materiality, [materiality - Glossary | CSRC \(nist.gov\)](#)
- 51 Bloomberg Law (2024), Corporate Governance, Overview - Shareholder Derivative Litigation Over Cyber Governance, [Corporate Governance, Overview - Shareholder Derivative Litigation Over Cyber Governance \(bloomberglaw.com\)](#)
- 52 ISS (2020), Equifax Agrees to High Profile Shareholder Settlement for \$149 Million, [Equifax Agrees to High Profile Shareholder Settlement for \\$149 Million | ISS \(issgovernance.com\)](#)





53 The New York Times (2019), Lessons for Corporate Boardrooms From Yahoo's Cybersecurity Settlement, [Lessons for Corporate Boardrooms From Yahoo's Cybersecurity Settlement - The New York Times \(nytimes.com\)](#)

54 European Parliament and Council of the European Union (2022), Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), [Directive - 2022/2555 - EN - EUR-Lex \(europa.eu\)](#)

55 Mayer Brown (2022), NIS2 Directive New Cybersecurity Rules Expected in the EU, [NIS2 Directive New Cybersecurity Rules Expected in the EU | Insights | Mayer Brown](#)

56 European Parliament and Council of the European Union (2019), Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), [Regulation - 2019/881 - EN - EUR-Lex \(europa.eu\)](#)

57 Ibid

58 Mason Hayes & Curran (2024), EU Cybersecurity Laws, [EU Cybersecurity Laws | Mason Hayes Curran \(mhc.ie\)](#)

59 European Parliament and Council of the European Union (2022), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, [Regulation - 2022/2554 - EN - DORA - EUR-Lex \(europa.eu\)](#)

60 US Securities and Exchange Commission (2023), Press Release: SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, [SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies](#)

61 UK Government Department for Science, Innovation & Technology (2024), Cyber Governance Code of Practice: call for views, [Cyber Governance Code of Practice: call for views - GOV.UK \(www.gov.uk\)](#)

62 WEF (2024), Global Cybersecurity Outlook 2024, [WEF Global Cybersecurity Outlook 2024.pdf \(weforum.org\)](#)

63 Ibid

64 Ibid

65 Ibid

66 Ibid

67 IBM (2024), Cost of a Data Breach Report 2024, [Cost of a Data Breach Report 2024 \(ibm.com\)](#)

68 ISS (2024) ISS-Corporate: U.S. Companies Face High Exposure to Third Party and Aggregate Cyber Risk, [ISS-Corporate: U.S. Companies Face High Exposure to Third Party and Aggregate Cyber Risk \(issgovernance.com\)](#)

69 Ibid

70 WEF (2024), Global Cybersecurity Outlook 2024, [WEF Global Cybersecurity Outlook 2024.pdf \(weforum.org\)](#)

71 Ibid

72 Gartner (2024), Gartner Survey Shows Rising Concern of AI-Enhanced Malicious Attacks as Top Emerging Risk for Enterprises for Second Consecutive Quarter, [Gartner Survey Shows Rising Concern of AI-Enhanced Malicious Attacks as Top Emerging Risk for Enterprises for Second Consecutive Quarter](#)

73 WEF (2024), Global Cybersecurity Outlook 2024, [WEF Global Cybersecurity Outlook 2024.pdf \(weforum.org\)](#)

74 The Guardian (2024), Company worker in Hong Kong pays out £20m in deepfake video call scam, [Company worker in Hong Kong pays out £20m in deepfake video call scam | Hong Kong | The Guardian](#)

75 Moody's (2023), 2023 Cyber Survey Highlights, [Moody's Cyber Survey \(moody's.com\)](#)

76 Proofpoint (2024), 2024 Voice of the CISO Report, [2024 Voice of the CISO \(nationalcioreview.com\)](#)

77 Proofpoint (2024), 2024 Voice of the CISO Report, [2024 Voice of the CISO \(nationalcioreview.com\)](#)

78 Ibid

79 ISC2 (2023), Cybersecurity Workforce Study, [ISC2\\_Cybersecurity\\_Workforce\\_Study\\_2023.pdf](#)

80 ISC2 (2022), Cybersecurity Workforce Study, [ISC2-Cybersecurity-Workforce-Study.pdf](#)

81 WEF (2024), Strategic Cybersecurity Talent Framework, [WEF\\_Strategic\\_Cybersecurity\\_Talent\\_Framework\\_2024.pdf \(weforum.org\)](#)

82 WEF (2024), The cybersecurity industry has an urgent talent shortage. Here's how to plug the gap, [Tackling cybersecurity's global talent shortage: Report | World Economic Forum \(weforum.org\)](#)

83 Ibid

84 UK Government Department for Science, Innovation, and Technology (2024), Cyber security skills in the UK labour market 2024, [Cyber security skills in the UK labour market 2024 - GOV.UK \(www.gov.uk\)](#)

85 WEF (2024), Global Cybersecurity Outlook 2024, [WEF\\_Global\\_Cybersecurity\\_Outlook\\_2024.pdf \(weforum.org\)](#)

86 European Union Agency for Cybersecurity (2024), ENISA Threat Landscape 2024, [ENISA Threat Landscape 2024 — ENISA \(europa.eu\)](#)

87 NCSC (2023), NCSC Annual Review 2023, [Case study: Russia - an acute and chronic cyber threat - NCSC.GOV.UK](#)

88 Ibid

89 Nili, Y., & Shapira, R. (2024). 'Specialist Directors' Yale J. on Reg., 41, 652, [Specialist Directors 41 Yale Journal on Regulation 2024](#)

90 Deloitte (2021), Role of cybersecurity in M&A, [PowerPoint Presentation \(deloitte.com\)](#)

91 Liberty Advisory Group (2024), Evaluating cyber risks in M&A due diligence, [Evaluating cyber risks in M&A due diligence - Liberty Advisor Group](#)

92 ISO (2022), ISO/IEC 27001:2022, [ISO/IEC 27001:2022 - Information security management systems — Requirements](#)

93 Iasme (2024), The benefits of Cyber Essentials certification, [Cyber Essentials - Cyber Essentials \(iasme.co.uk\)](#)

94 NIST (2024), Cybersecurity Framework, [Cybersecurity Framework | NIST](#)

95 Secureframe (2023), SOC 2 Type II Compliance: Definition, Requirements, and Why You Need It, [SOC 2 Type II Compliance: Definition, Requirements, and Why You Need It | Secureframe](#)

96 Ifac (2011), International Standard on Assurance Engagements (ISAE) 3402, [IAASB General Template \(Portrait\) \(ifac.org\)](#)

97 Syteca (2024), The 7 Industries Most Vulnerable to Cyberattacks, [The 7 Industries Most Vulnerable to Cyberattacks | Syteca](#)

98 Black Kite (2023), 2023 Third Party Breach Report, [third-party-breach-report-2023.pdf \(blackkite.com\)](#)

99 IBM (2024), Cost of a Data Breach Report 2024, [Cost of a Data Breach Report 2024 \(ibm.com\)](#)

100 Fair Institute (2024), How Material is That Hack?, [Hack Overview - How Material is That Hack](#)





101 Ibid

102 Ibid

103 IBM (2024), Threat Intelligence Index 2024, [IBM Security X-Force Threat Intelligence Index 2024](#)

104 IBM (2024), Cost of a Data Breach Report 2024, [Cost of a Data Breach Report 2024 \(ibm.com\)](#)

105 Ibid

106 Ibid

107 UpGuard (2023), Supply Chain Ransomware Attack Impacts Semiconductor Manufacturer, [Supply Chain Ransomware Attack Impacts Semiconductor Manufacturer | UpGuard](#)

108 Ibid

109 Ibid

110 IMF (2024), Global Financial Stability Report, [The Last Mile: Financial Vulnerabilities and Risks \(imf.org\)](#)

111 IBM (2024), Cost of a Data Breach Report 2024, [Cost of a Data Breach Report 2024 \(ibm.com\)](#)

112 IMF (2024), Global Financial Stability Report, [The Last Mile: Financial Vulnerabilities and Risks \(imf.org\)](#)

113 CSO (2020), Equifax data breach FAQ: What happened, who was affected, what was the impact?, [Equifax data breach FAQ: What happened, who was affected, what was the impact? | CSO Online](#)

114 CNBC (2019), Equifax just became the first company to have its outlook downgraded for a cyber attack, [Moody's downgrades Equifax outlook to negative, cites cybersecurity \(cnbc.com\)](#)

115 CFO Brew (2024), Cyberattacks can hurt your company's creditworthiness, [Cyberattacks can hurt your company's creditworthiness \(cfobrew.com\)](#)

116 FCA (2023), Financial watchdog fines Equifax Ltd £11 million for role in one of the largest cyber security breaches in history, [Financial watchdog fines Equifax Ltd £11 million for role in one of the largest cyber security breaches in history | FCA](#)

117 IBM (2024), Threat Intelligence Index 2024, [IBM Security X-Force Threat Intelligence Index 2024](#)

118 Syteca (2024), The 7 Industries Most Vulnerable to Cyberattacks, [The 7 Industries Most Vulnerable to Cyberattacks | Syteca](#)

119 CEPA (2018), Cybersecurity in the energy sector: what does it mean for network regulation?, [Cybersecurity in the energy sector | CEPA](#)

120 ISS (2023), Cybersecurity Threats to Critical Energy Infrastructure: Business Continuity in a Changing Geopolitical Environment, [Cybersecurity Threats to Critical Energy Infrastructure: Business Continuity in a Changing Geopolitical Environment \(issgovernance.com\)](#)

121 Cisco (2021), Key Takeaway from the Colonial Pipeline Attack, [Key Takeaway from the Colonial Pipeline Attack - Cisco Blogs](#)

122 TechTarget (2023), The 10 biggest ransomware attacks in history, [The 10 biggest ransomware attacks in history | TechTarget](#)

123 Cisco (2021), Key Takeaway from the Colonial Pipeline Attack, [Key Takeaway from the Colonial Pipeline Attack - Cisco Blogs](#)

124 ICGN (2023), Systemic Stewardship & Public Policy Advocacy Toolkit September 2023, [Systemic Stewardship & Public Policy Advocacy Toolkit](#)

### Disclaimer

The information contained in this document is provided solely for informational purposes and has been produced by Railpen Limited working in collaboration with Royal London Asset Management Limited. While every effort has been made to ensure the accuracy and completeness of the information, no representations, or warranties (whether express or implied) are made about the completeness, accuracy, reliability, suitability, or availability of the information contained herein. This document does not constitute legal, financial, or professional advice and should not be relied upon as such. Railpen Limited and Royal London Asset Management Limited disclaims any and all liability for any loss or damage, whether direct, indirect, consequential, or otherwise, arising from the use or reliance on the information contained herein.

The views expressed within this document are those of Railpen Limited and Royal London Asset Management Limited at the date of publication, which are subject to change. The information contained within this document does not constitute investment advice and should not be treated as such.

Railpen Limited is a wholly owned subsidiary of Railways Pension Trustee Company Limited, registered in England and Wales under company number 02315380 whose registered office is at 100 Liverpool Street, London, EC2M 2AT.

[www.railpen.com](http://www.railpen.com)

Royal London Asset Management Limited is a subsidiary of The Royal London Mutual Insurance Society Limited, registered in England and Wales under company number 02244297 whose registered office is at 80 Fenchurch Street, London, EC3M 4BY.

Authorised and regulated by the Financial Conduct Authority, firm reference number 141665.

[www.RLAM.com](http://www.RLAM.com)





✉ 100 Liverpool Street, London, EC2M 2AT  
@ SO@railpen.com

**RAILPEN**

✉ 80 Fenchurch Street, London, EC3M 4BY

