For professional clients only, not suitable for retail clients.

Cyber security engagement phase 3

January 2023

ROYAL LONDON
ASSET MANAGEMENT

Cyber security engagement phase 3

How we monitor cyber risk in our portfolios

Cyber security is both an investment performance and regulatory risk and as responsible investors we believe monitoring this risk is of vital importance. However, this area is challenging to assess and monitor due to a lack of public disclosures, sensitivity, and the complicated nature of the topic.

We have found engagement invaluable in uncovering information to help us monitor this risk. In 2022 we launched phase 3 of our cyber security engagement programme, building on the previous two phases of engagement which started in 2020. In phase 3 we expanded the scope of the programme to include policy advocacy, assessed companies against our investor expectations and discovered examples of best practice.

Why are we engaging on cyber security?

The threat of a cyberattack is ever present:

The UK's National Cyber Security Centre (NCSC) found that 39% of UK businesses identified a cyber breach or attack in the past 12 months and many more appear to not be adequately managing this risk[1]. There has been an increase in corporate reliance on technology, particularly due to hybrid working, and against a backdrop of increased geopolitical tensions, this has amplified our concerns around cyber security risks as investors.

Cyber security practices affect business and investment performance:

Research has found that cyber security breaches negatively affect share price performance, where six months after a breach the average share price performance typically falls 3% against the NASDAQ[2]. This partly reflects the fines, loss of consumer confidence and revenues, and reputational harm corporate targets experience because of a cyber security breach. Another paper found that one month after a cyberattack, bondholders lost approximately 2% of their wealth[3]. More positively, the World Economic Forum Cyber security Outlook 2022[4] found that prudent management of cyber security risk contributes to business outperformance.

Regulatory risk from more stringent regulation:

Globally regulators are recognising and responding to cyber security risks by focusing on improving systemic cyber-resilience through regulation. This increases the regulatory risk for investors because companies that are unprepared for the more stringent regulation are likely to receive fines or incur large costs due to disorderly management. As a result, we believe that continuing to engage with companies is important to ensure management will focus on cyber risk management.

Public disclosures are limited:

Due to the sensitivity of the matter companies are not inclined to disclose details on their cyber security systems, policies, and practices. This may be one of the few areas in ESG where we recognise, alongside the views of our holding companies, that increasing disclosure may not be in the best interests of the companies or their investors. In fact, excessive cyber security disclosures could make companies more susceptible to attacks.

With this in mind, and as responsible investors, we believe robust management of cyber security is essential. Given the confidentiality of cyber security policies and practices, we have found engaging with our investee companies invaluable in building information to help us monitor this risk.

The evolution in our engagement approach:

In 2020, we launched our engagement on cyber security with a selection of our investee companies as part of our broader 'innovation, technology & society' engagement theme. Since then, we have conducted three phases of the engagement where we targeted and sent letters to over 49 companies and had meetings or received detailed written responses from 69% of them.

Each phase represents an evolution of our approach — we have targeted different companies for each phase and evolved the aims of the engagement and key asks we made of companies we engaged with. As we met with more companies, our understanding of best practice has progressed, and we incorporated learnings from previous phases to further develop the engagement programme.

1 Cyber Security Breaches Survey 2021 - GOV.UK (www.gov.uk)|
2 Bischoff, Paul. 2021. How data breaches affect stock market share prices. Comparitech. https://www.comparitech.com/ blog/information-security/ data-breach-share-price-analysis/#NASDAQ_benchmark_validation (link as of 23/11/21)
3 Cyberattacks and Impact on Bond Valuation by Subramanian R. Iyer, Betty J. Simkins, Heng Emily Wang :: SSRN
4 Economic Forum Cyber security Outlook 2022

Despite the engagement programme continuously evolving with our learnings, the aims of the programme have remained consistent since the beginning. These include:

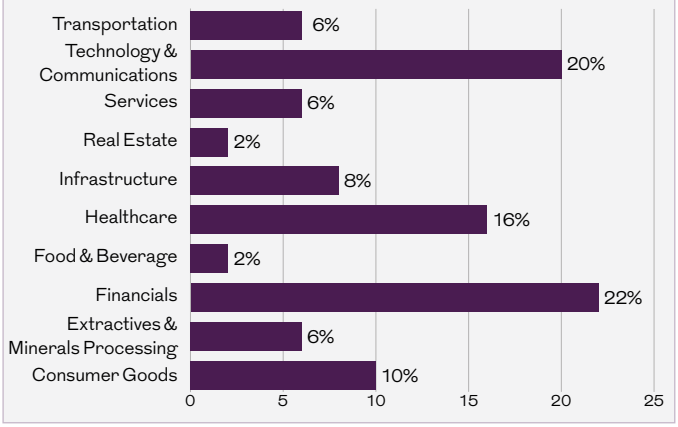
- Monitor cyber security risk in our portfolios.
- Gain insights that are not in the public domain[5].
- Use this information to assess management of cyber security risk against our investor expectations.

Companies targeted:

Initially in phase 1 we targeted sectors identified specifically as 'at risk' by the European Cyber security Directive including healthcare, retail, and utilities. We found that the highest risk sectors often have the most comprehensive oversight from regulators. Given this, in phase 2 and 3 instead of focusing on specific sectors we focused on companies in any sector which are at higher risk to cyber-attacks due to their exposure to threat, technology dependency, and service criticality.

In phase 1 we predominantly focused on equity holdings. In the following phases we included more issuers of debt instruments, to better evaluate cyber security risk within our credit portfolios, as the issue is equally material to both asset classes.

Sectors targeted across the 3 phases of engagement.



Source: RLAM (all figures are subject to rounding)

Investor expectations:

As noted previously, we have evolved our understanding of cyber risk and how to reduce it. For example, in phase 1 a key area of focus of letters and meetings was the publication of robust detailed cyber security policies. Through our discussions we found that companies were reticent to disclose their cyber security policies and heard from experts of the risk of publishing even seemingly benign cyber security details due to the increasing risk of cyber-attacks.

We realised that dialogue rather than increasing general disclosures may be in the best interests of investors. Consequently, in phase 2 we redirected our efforts towards uncovering the leadership and resources that underpin the governance and risk management of cyber security risk. This provides reassurance that appropriate policies, systems and controls are in place without the need for disclosure or information.

We used the learnings from phase 1 and 2 to inform the publication of our **investor expectations** at the end of 2021. Alongside the focus on governance and risk management the minimum expectations focus on areas of enhanced risk such as corporate culture, corporate action and third parties. The advanced practices are informed by examples of best practice we have encountered. We have used these expectations as the basis of our letters and meetings in phase 3 to gain the information necessary to assess how a company performs against these investor expectations.

Minimum expectations:

- Risk identification and oversight at board level
- A nominated Chief Information Security Officer (CISO) with supporting resources
- Inclusion of cyber covenants in supplier contracts and effective due diligence
- Inclusion of cyber considerations in inorganic growth strategies including in the due diligence and integration phases
- Timely disclosure of cyber security breaches
- Disclosures about a cyber-resilient culture, to include tailored training across the workforce

Advanced practices

- Inclusion of information security and cyber-resilience in executive compensation KPIs
- Use of NIST (National Institute of Standards and Technology) Cyber security Framework as a reference for cyber security risk management
- ISO 27000 for all operations
- Evaluation of cyber security in board effectiveness review

5 However, our preference is not to be made insiders.

Policy advocacy:

During our engagement it was difficult to assess the timely disclosure of material cyber security breaches as part of our investor expectations. Companies were reticent about disclosing information as regulation is limited and many breaches do not require disclosure. In phase 3, we have adapted our approach to include supporting relevant and appropriate regulation.

The U.S. Securities and Exchange Commission (SEC) proposed a new rule[6] this year which would enhance and standardise cyber security disclosure by public companies. This includes timely disclosure of material incidents and other areas covered in our investor expectations, such as the Board of Directors' oversight of cyber security risk. We co-signed a response to the SEC supporting the proposal and highlighting the alignment between our experience and the Commission's proposal. We welcome regulators' increased scrutiny on cyber security worldwide and will continue to support regulation which helps investors monitor this risk.

Regulators are recognising and responding to cyber security risks by focusing on improving systemic cyber-resilience. The proposed legislations, such as that in the UK and the US, should increase our ability to assess cyber security risk and identify good and poor performers. In addition, this increases the regulatory risk that companies without adequate cyber security risk management face censure and fines from regulators or incur large costs by disorderly management of the risks. The alignment between the focus of the regulators and our investor expectations on governance, third-party risk management and timely disclosure of cyber security breaches re-affirms the importance of these areas in cyber security risk management.

Phase 3 Engagement Process

In 2022, we launched phase 3 of our cyber security engagement programme and identified twelve companies in our portfolios that may be at higher risk to cyber-attacks due to their exposure to threat, technology dependency, and service criticality. Of the 12 companies we contacted, only one was unresponsive and one requested we delayed our meeting as they were conducting an internal review on ESG disclosures.

We used information gained from our discussions to evaluate how each company performed against our expectations. We grouped these around common themes and used them to assess each company ahead of and after our engagement meetings.

Engagement Learnings

Given the sensitivity of cyber security issues we have found there is significant value from meeting with companies beyond relying solely on desk-based research. These engagement learnings have been invaluable in aiding our ability to accurately consider ESG risks.

In our preliminary analysis, there have been instances where we have identified areas of concern and it was only by having a transparent dialogue with the companies that we were able to understand and assess whether there were sufficient mitigations in place. The below on the following page are examples of learnings noted.

Regulatory updates:

UK:

- Proposal published to expand the scope of The Security of Network & Information Systems Regulations (NIS) to include third party providers of information technology services and to require better cyber incident reporting by large companies[7].

Europe:

- The European Union's Digital Operational Resilience Act (DORA) came into effect which introduces sector specific regulation on cyber incident reporting, testing and third-party risk management for financial services firms[8].
- The EU agreed measures for a high common level of cyber security across the union with the Network and Information Security 2 (NIS2) Directive[9].

6 https://www.sec.gov/rules/proposed/2022/33-11038.pdf
7 https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience#:~:text=An%20expansion%20of%20the%20NIS,on%2Dgoing%20incident%20reporting%20costs.
8 https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/
9 https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

Transportation Company1 [10]

We were initially unsure about the comprehensiveness of the board oversight of cyber security from the parent of this private transport company. However, when the CEO and CFO both attended our engagement meeting they were able to demonstrate that they were very knowledgeable on the subject. From the engagement, we were satisfied that the current Executive Board provides sufficient oversight through monthly updates from operational committees and are actively demonstrating best practice. This combined with the evidence of good and best practice in other areas, notably culture and training, led us to conclude that the lack of evidence of good board oversight was mitigated by exceptional performance elsewhere.

Transportation Company 2

This transportation company's digital interfaces are closely linked to a key user and whilst the company themselves had no recent cyber and technology issues the user has had several. As a result, we expressed concern relating to the vulnerabilities from third parties and wanted to reiterate the importance of a secure information perimeter. From the meeting, we discovered this company was working closely with the user to improve their cyber-resilience and there has been an improvement over the last year.

The company also receives extensive oversight from government agencies and the regulator and has been working closely with them to improve the user's cyber security. Prior to the meeting we were dissatisfied with the company's performance regarding its suppliers and Mergers and Acquisitions (M&A), given the lack of information on measures taken to mitigate the user's poor historical cyber security performance. However, given the information gained from our meeting and evidence of good practices we improved our sentiment with regard of those two issues despite the historical issues.

Best Practice

We have been able to identify examples of best practice from speaking to the 12 companies during the engagement, as summarised below.

'Friendly' cyber-attacks:

We uncovered several examples of best practice on how companies prepared themselves for cyberattacks. Several companies had an in-house 'ethical' hacking team, separate from the cyber security team, who try and infiltrate the companies' IT systems. A healthcare company had an innovative 'bug bounty' programme in which hackers were invited to find vulnerabilities in their website and paid for their exploits. Actively seeking 'friendly' cyber-attacks enable companies to avoid group think on cyber security and resolve vulnerabilities before bad actors can exploit them.

Training and culture:

Employees are often the gateway for hackers into IT systems and are one of the most vulnerable parts of a company's cyber defences. We identified a few examples of best practice in how companies maintain a cyber aware culture at all levels of the organisation. Transportation Company 1 told us how they specifically targeted senior leadership in simulated attacks and changed employee chat interfaces and the website as part of the simulated attack. A financial company 'gamified' cyber security training with different badges employees can achieve; ensuring all employees continue to be engaged in guarding against the threat requires creativity and we were impressed by many of the approaches taken.

Collaboration:

A common theme we discovered was the value companies gained from collaboration both with peers and with government bodies. Another financial company was a founding member and host of the Cyber Defence Alliance which shares best practice and threat intelligence with other UK banks. Additionally, Transportation Company 1 participated in external industry and government committees such as the Rail Cyber Security Committee and the Rail Information Exchange (part of National Cyber Security Centre). Both companies emphasised the step change increase in collaboration following the Russian invasion of Ukraine and the subsequent heightened risk of cyber-attacks. There are large benefits from this type of collaboration for preparedness and risk mitigation. Whilst collaboration is not part of our investor expectations, we found that best practice in this area correlates with best practice in cyber security resourcing. It may be that a well-resourced cyber security team is necessary to actively collaborate externally, or it may be that a company that prioritises cyber security risk management recognises the importance of both resourcing and collaboration.

Further Resources:

- NCSC: Cyber Security Toolkit for Boards
- WEF: Global Cyber security Outlook 2022
- NCSC: Cyber Essentials

10 We have anonymised the names of the investee companies because the information shared was in confidence with the collaborative engagement investors.

Conclusion

Overall, this engagement programme reassured us that the targeted companies are broadly meeting our investor expectations. It reaffirmed the value of direct conversations with companies given the lack of public disclosures.

Importantly, we have also been reassured that companies are focusing resources on cyber security and were pleased to hear the value companies gained from these conversations in terms of better understanding investor's expectations.

For professional clients only, not suitable for retail clients.

Contact us

For more information, please contact us
Royal London Asset Management
55 Gracechurch Street, London, EC3V ORL
020 7506 6500
esg@rlam.co.uk

rlam.com

Issued in January 2023 by Royal London Asset Management Limited, 55 Gracechurch Street, London, EC3V ORL. Authorised and regulated by the Financial Conduct Authority, firm reference number 141665. A subsidiary of The Royal London Mutual Insurance Society Limited.

Ref: PDF RLAM PD 0124