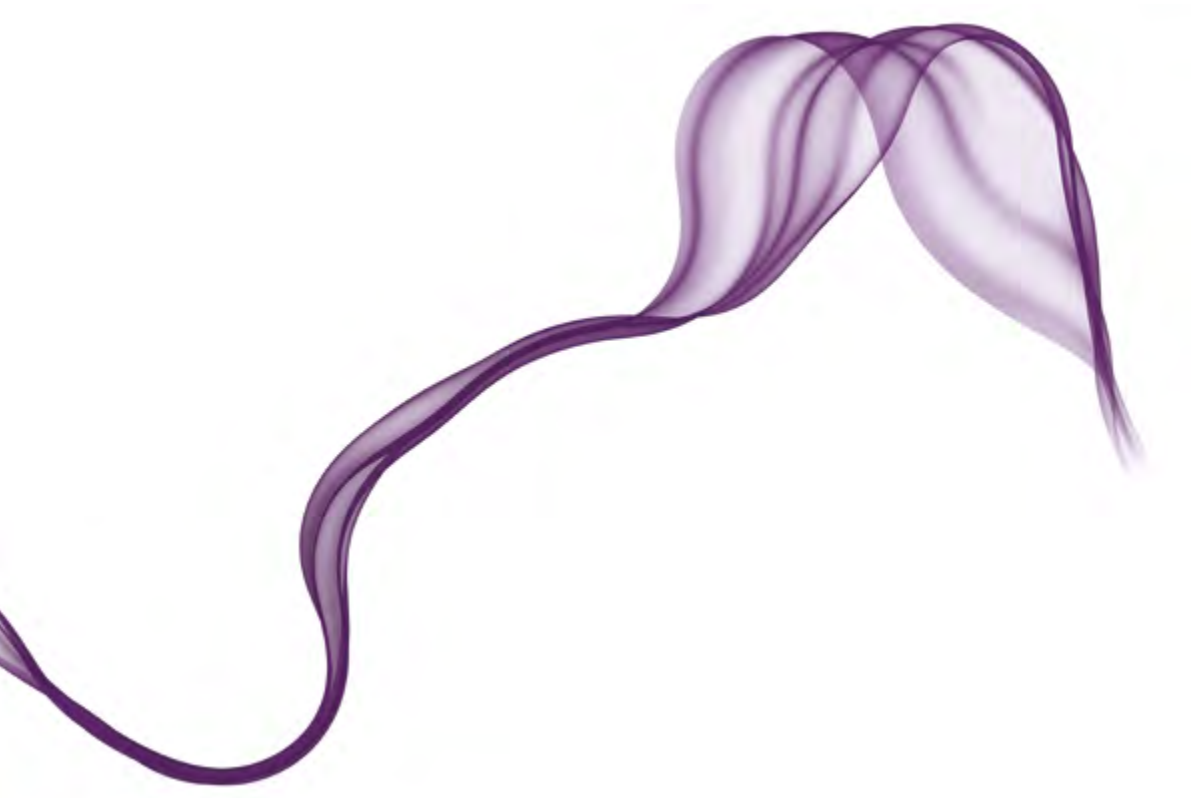
For professional clients only, not suitable for retail clients.

Cybersecurity engagement update

December 2021

ROYAL LONDON
ASSET MANAGEMENT

Contents



Executive summary

Since last reporting the progress of our cybersecurity engagement efforts, it has been hard to ignore the steady increase of cyber-attack and ransomware stories making media headlines and climbing the agendas of various governments. The rise in media attention has only further highlighted the vulnerability – exacerbated by COVID – and the need for enhanced protection of critical infrastructures including electricity grids, nuclear power generators, pipelines, health systems and stock exchanges.

From our dialogue with companies to date, a few trends are clear; companies are investing more in cyber-resilience and because of the sensitivity of the matter, they are not inclined to disclose more about their systems publicly. This may be one of the few areas in environmental, social, and governance (ESG) where we recognise, alongside the views of our holding companies, that increasing disclosure may not be in the best interest of the companies or their investors. In fact, excessive cybersecurity disclosure could make companies more susceptible to attacks. Despite this revelation, we still have found this engagement very insightful in providing us with the details and comfort that this increasing risk is not being overlooked.

What do we consider the minimum disclosure requirements to be?

- Risk identification and oversight at Board level.
- A nominated Chief Information Security Officer (CISO) with supporting resources.
- Embedding of cyber requirements in contracts and suppliers' due diligence and in the strategies for corporate action and M&A.
- Timely disclosure of cybersecurity breaches.
- Appropriate resources and culture/training across the workforce.

Introduction

In spring 2020, at the height of the COVID-19 pandemic, an innocent software update ping caused havoc across businesses and governments globally. SolarWinds, a US software company was the target of a cyber-attack which cascaded down to computer networks across North America, Europe, Asia and the Middle East. The attack affected a wide range of organisations, from governments to technology and telecoms, along with other entities and their value chains. The extent of this attack resulted in increasing concerns about national security and the risk faced by most businesses, even those with world-class cybersecurity teams.

Whether the Sunburst hack (the name given by researchers) described above was the work of a nation or criminal hackers, is still unknown. However, what we do know is that such hackers are still very much active, as has been seen in the case of CD Projekt in February this year[1], Colonial Pipeline in May[2], and JBS just a month after[3].

Criminal hackers focus on short term financial gain using techniques such as ransomware, Denial of Service (DoS), phishing, clickjacking etc., to steal financial information, extort money from their targets, and other crimes. Typically, criminal hackers will exploit preventable security vulnerabilities. Hackers associated with governments have different motives and are mainly interested in espionage, and the theft of information and intellectual property.

Because many of the criminal hacks on private companies may involve governmental departments in their resolution or may even expose governments to enhanced risk, more governmental intervention could be expected. This has been the case in the US[4] for example, where the Biden administration issued an executive order establishing a "zero trust" on supply chains and called for action to address growing cybersecurity threats. This seems to have been followed by a commitment by some hackers to keep critical infrastructures off bounds – the extent to which we can trust the assurances of criminals is another matter, and how can we be sure they could control their affiliates?

This all emphasises the importance for companies to have strong and dynamic security strategies, particularly those that run on legacy, broad and complex systems and/or are exposed to well-trusted third-party systems or software.

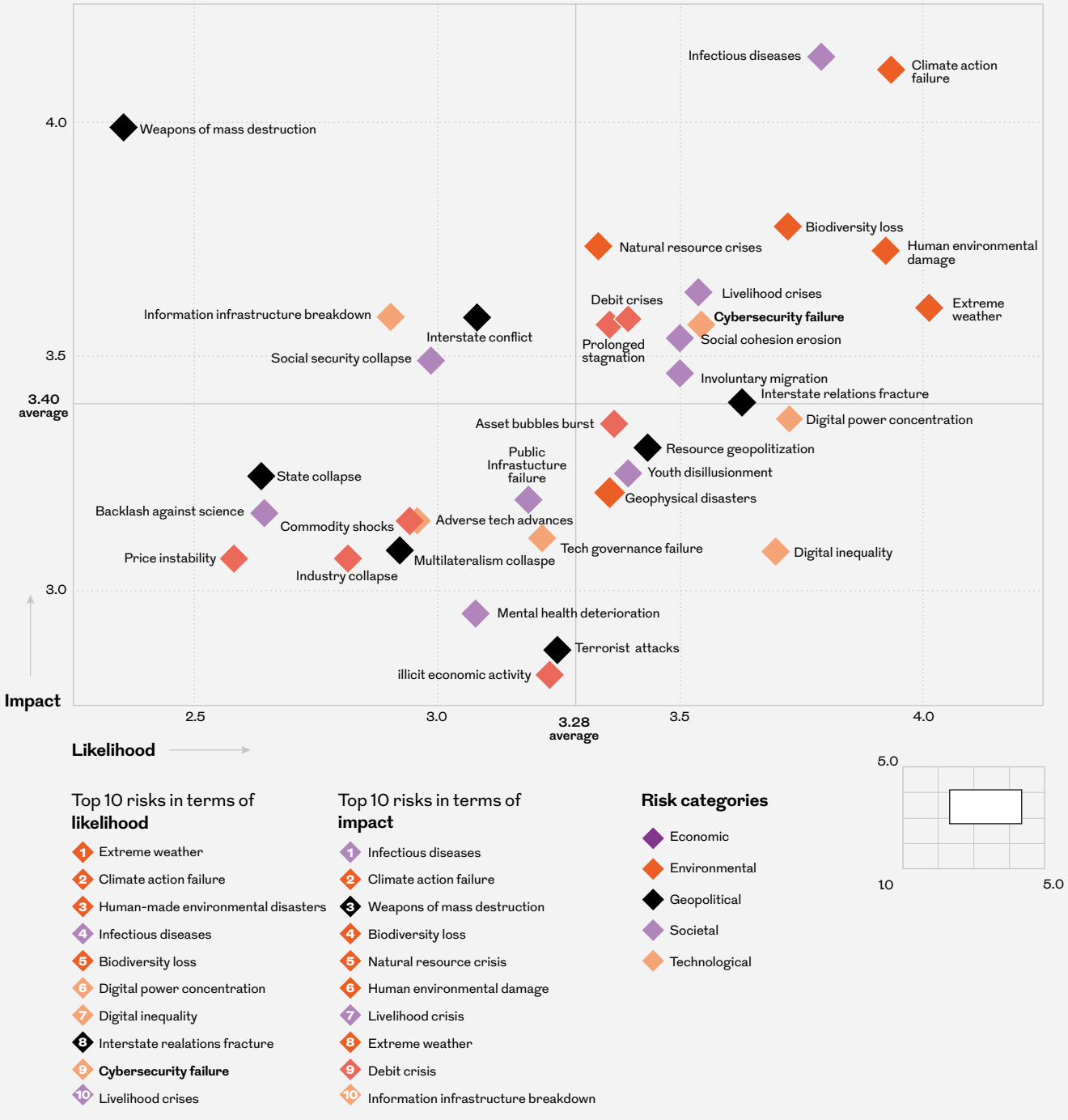
We initiated our critical engagement with holding companies on cybersecurity in 2020 as part of our broader "innovation,

1 CD Projekt, a Polish gaming company, was the victim of a targeted cyberattack and threatened with leaking its source codes and internal documents. The company stated that it would not give in to the demands or negotiate with the attackers, being aware that the compromised data would be ultimately released.
2 Colonial Pipeline, an American oil pipeline system suffered a ransomware attack that impacted its digital systems. Its operations were halted and with FBI's assistance the requested ransom, around USD4.4m was paid, half of which was later recovered in bitcoins.
3 JBS, the world's largest meat processor reported a cyberattack that crippled its servers in North America and Australia and resulted in a ransom payment of around USD11m. The Australian government and Federal policy got involved to resolve the issue.
4 Executive Order on Improving the Nation's Cybersecurity | The White House; FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity | The White House

technology & society" engagement theme, just as COVID-19 was shutting down offices and displacing a large proportion of the global workforce to remote locations. The widespread use of technology and the continuous reliance of business on digital access exacerbated the cybersecurity risk to companies of all sizes and sectors.

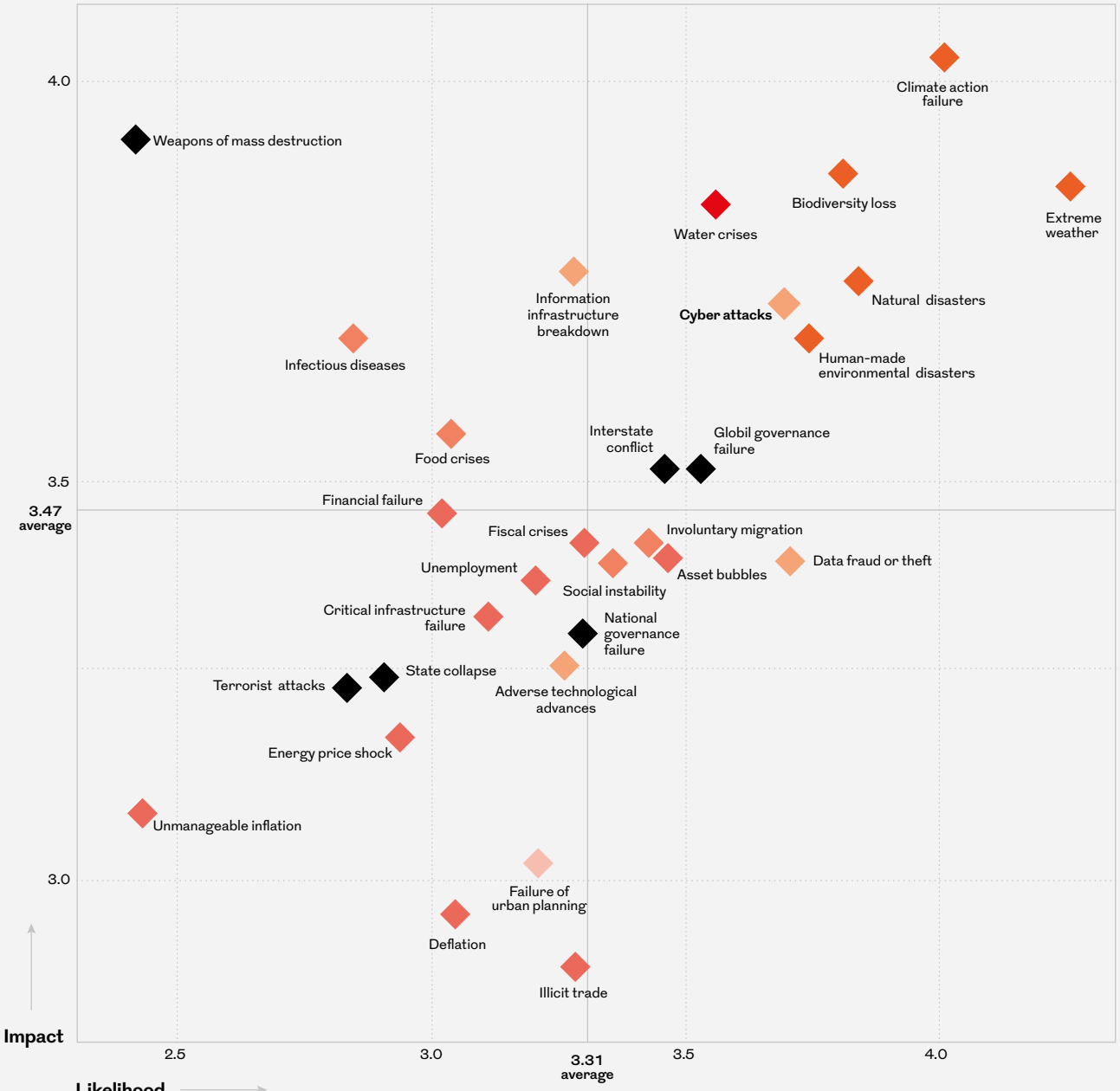
This engagement priority follows the World Economic Forum's consistent categorisation of cybersecurity as one of the most likely risks to occur, and with a considerably high global impact.

Figure 1: The Global Risks Landscape 2021



Source: World Economic Forum Global Risks Perception Surveys 2019 – 2021.

Figure 2: The Global Risks Landscape 2020



Top 10 risks in terms of **likelihood**

1. Extreme weather
2. Climate action failure
3. Natural diasters
4. Biodiversity loss
5. Human-made environmental disasters
6. Data fraud or theft
7. **Cyber attacks**
8. Water crises
9. Global Governance failure
10. Asset bubble

Top 10 risks in terms of **impact**

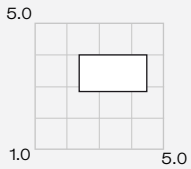
1. Climate action failure
2. Weapons of mass destruction
3. Biodiversity loss
4. Extreme weather
5. Water crisis
6. Information infrastructure breakdown
7. Natural disasters
8. Cyber attacks
9. Human-made environmental disasters
10. Infectious diseases

Risk categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Source: World Economic Forum Global Risks Perception Surveys 2019 – 2021.

Figure 3: The Global Risks Landscape 2019



Top 10 risks in terms of **likelihood**

1. Extreme weather
2. Failure of climate-change mitigation and adaptation
3. Natural disasters
4. Data fraud or theft
5. **Cyber attacks**
6. Man-made environmental disasters
7. Large scale involuntary migration
8. Biodiversity loss and ecosystem breakdown
9. Water crises
10. Asset bubbles in a major economy

Top 10 risks in terms of **impact**

1. Weapons of mass destruction
2. Failure of climate-change mitigation and adaptation
3. Extreme weather events
4. Water crisis
5. Natural disasters
6. Biodiversity loss and ecosystem breakdown
7. Cyber attacks
8. Critical Information infrastructure breakdown
9. Man-made environmental disasters
10. Spread of Infectious diseases

Risk categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Source: World Economic Forum Global Risks Perception Surveys 2019 – 2021.

Our focus in the second phase of this engagement was to rekindle our outreach with companies that were unresponsive during phase 1, and to initiate dialogue with new companies, particularly issuers of debt instruments, to better evaluate the risk in our credit portfolios.

In this second phase we reached out to 24 companies, half of which we were able to speak with. General findings from these conversations point to the value of engagement in understanding the risk mitigation measures that our holdings have in place and which are not obvious from their public disclosure on many occasions.

We found additional elements of best practice (see Appendix) including the certification to ISO27000 for wide operations – not just to satisfy a government contract. Companies are also disclosing their use of the National Institute of Standards and Technology (NIST) cybersecurity framework as a reference for controls to prevent, detect and address cyber security threats. Furthermore, some companies have included the cost of enhanced cybersecurity in their analysis of operating expenses, and their positive contribution to public policy development. Finally, we found further inclusion of technology (and cybersecurity) considerations in board compensation and effectiveness reviews.

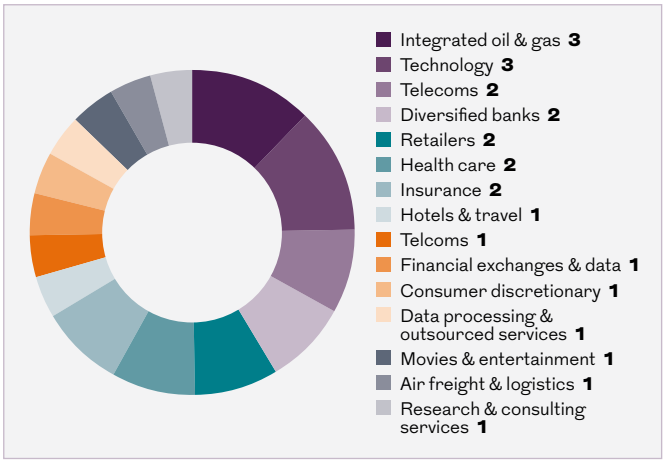
Figure 4: NIST Cybersecurity Framework Overview

General progress

During the second phase of our engagement on cybersecurity we approached 24 companies. In this second iteration we sought a mixture of debt and equity issuers as we found the issue is equally material for both asset classes.

The sector distribution was more heterogeneous in this second round. However, we still focused on sectors that are perceived to be at higher risk by nature as critical infrastructures or services, or by exposure through "threat surfaces" or multiple access points.

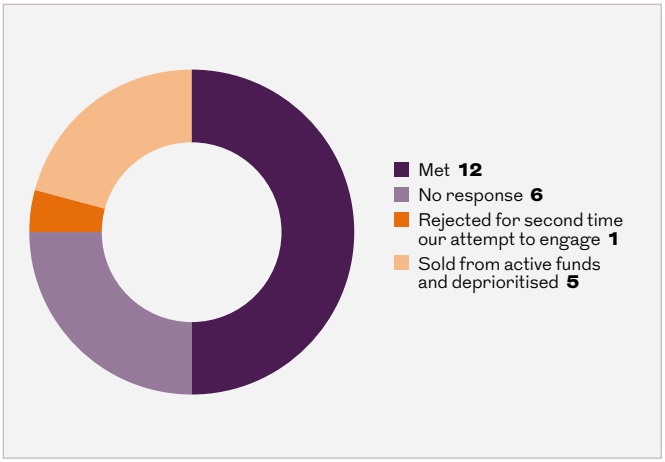
Figure 5: Cybersecurity sector distribution



Source: RLAM as at October 2021.

At the time of writing this report, half of the companies contacted responded to our outreach and we took opportunities to meet with all of them. Only one company, which had acknowledged receipt during phase 1 but declined to engage, still openly rejected our attempts to establish a dialogue. During the period, we exited active positions in some of the issuers in scope. We prioritised our active holdings, which we find maximises our influence.

Figure 6: Engagement progress



Source: RLAM as at October 2021.

The quality of engagements with the majority of companies was very good, with some inviting Chairpersons and C-suite executives to join the meetings, while others brought their Chief Information Security Officers (CISO) and other technical experts. In both instances, we found the discussions were very rich and insightful.

The issuers in sectors linked to financial activity showed a great deal of awareness and advanced systems, in part due to the scrutiny they are under resulting from their systemic importance. But in general, with few exceptions, we found that companies in the financial sector were well-equipped to react to potential cyber threats, and to minimise their impact, should they occur.

Examples

The AA (Automobile Association)

Engagement Type: Meeting

Outcome: Positive

Details:

We found that the AA has already disclosed substantial information in the public domain. The risk committee oversees cyber risk and reports to the board four times a year. The company describes the following in detail: how cyber threats are a principal risk, how they mitigate against risks, what changes are likely in the year ahead, the impact of these changes, the likelihood of attacks, and the trends in the roadside assistance and insurance segments of its business.

During the meeting, the company disclosed its improvement programme installed to measure the performance of its defences and shared some of the metrics it reports against, including patch and vulnerability levels, ticket levels, and the speed of resolutions. The company confirmed that it is covered by a comprehensive insurance policy which includes protection against cyber-attacks. It also seeks expertise from various external advisors, but acknowledged that this is an immature industry. To keep informed of developments, the company remains involved in various forums, such as the UK Cyber Security Information Sharing Partnership (CiSP).

The AA publishes a certification for AA Drive Tech (Cyber Essentials), however they explained at our meeting that this was obtained as a requirement in contracts from law enforcement clients. When we asked about the extension to the group, we were informed that this is a difficult standard to maintain. Instead, the AA expected to achieve ISO 27001 certification for its Roadside segment by mid-March 2021.

ANSYS Inc

Engagement Type: Meeting

Outcome: Positive

Details:

Our meeting with ANSYS was well attended and led by the Senior Director for Cybersecurity. There was ample time for discussion and the company was open to learn more, aware of the growing interest from investors.

The company confirmed it would be hesitant to publish a standalone cybersecurity policy amidst concerns about striking the right balance between openness & transparency and keeping hackers at bay.

ANSYS provided us with additional insights into its cyber governance, notably the existence of a cross-functional cyber committee chaired by the CFO and general counsel. The company's audit committee however provides ultimate oversight and receives quarterly updates from the cyber steering committee against the company's cybersecurity roadmap. The CEO receives regular briefings from the cyber steering committee as well. This body meets on a monthly basis and comprises all stakeholders at C-suite level. The senior director for cybersecurity also holds monthly meetings with the CEO.

While there is no cyber director or committee at board level, the company feels there is a lot of technical expertise and experience distributed across the firm. All directors undertake cyber training during the induction process and are considered "fluent" on current issues. The company is considering our suggestion to embed cyber-related KPIs in executive compensation.

The Cybersecurity Maturity Model Certification (CMMC) will be limited to the defence segment of the business. The team also informed us it was finalising its System and Organization Controls 2 (SOC 2) report. In terms of metrics, the company uses its Microsoft Secure and Exposure Scores, alongside National Institute of Standards and Technology (NIST) maturity ratings provided by a third-party assessor (PwC).

Best practice:

The company's long-term goal is to achieve ISO 27001 certification across the whole organisation. This provides the best framework for cybersecurity policies. The NIST framework is more focused on cybersecurity controls.

Center Parcs

Engagement Type: Meeting

Outcome: Positive

Details:

After a failed attempt to meet the company due to the impact of employee furloughs, we were able to have a very productive discussion with Center Parcs as the UK relaxed the early 2021 lockdown. Private companies have less drivers for disclosure and Center Parcs is no different. However, we were very satisfied with the level of participants at the meeting and their knowledge of the technical, risk management and governance aspects associated with cyber resilience.

During our discussion we addressed how little information there was in the public domain. Center Parcs endeavour to publish their ESG framework in upcoming months which will include cybersecurity risk as part of their governance disclosure. The company's board oversees all risks, with board level working knowledge of cybersecurity and other risks. An information security officer has been in place for a number of years in the business. It was made clear that the company's approach is not to be complacent, but to mitigate –

if not remove – cyber risk while acknowledging this is a very fast-moving area. The company acknowledges that their third-party relationships are exposed to the threat of a cyber breach and it endeavours to remain up to speed with the systems and measures used.

Reports on cybersecurity to the operating board occur monthly. There is a separate risk committee (audit) which also reviews operational and cyber risk on a quarterly basis. The company's risk wheel and balanced scorecard take all systems and process into account. Risk evaluation is followed by capital for security budget. Simulations are used to address cyber and data loss scenarios. The board participates and receives progress reports. The company has a good record of its past simulations and follow up systems on patches and configuration changes.

Best practice:

A system of continuous monitoring and improvement includes continuous simulations. This is mandated and reported as per the insurance agreement.

Deutsche Post

Engagement Type: Meeting

Outcome: Neutral

Details:

The company provided details of its response to multiple attacks on container shipping and logistics firms. In Deutsche Post's case, these hacking attempts were caught early on, preventing the spread to networks.

With the complexities like logistics, global footprint, external systems and customs clearing systems, cyber security is a topic of regular discussion and a top priority for the CEO.

The company has strengthened its systems with the help of a dedicated team and drills, and training for the entire organisation. A recent group audit review revealed encouraging results.

With regards to risk management, the company confirmed it has a Chief Information Security Officer (CISO) which oversees the risk and control systems that manage cyber risk with a quantifiable pseudo-scientific focus on counter measures, redundant systems, and tests.

The company confirmed its internal cybersecurity culture includes mandatory info security training for its staff, simulations, and is supported by external experts.

Note that the outlook of this engagement was deemed 'neutral' because we did not receive the same level of insight provided by the other companies we engaged with.

Intuit

Engagement Type: Meeting

Outcome: Positive

Details:

The company has ISO 27001 for a portion of its operations with the intention to cover the full business over the next few years. Intuit's cyber risk model is also supported by an external framework, and an annual information security forum. This is reported to the board regularly and formally on a quarterly basis.

Due to the nature of the business, the company's board has relevant experience (technology, security and anti-fraud). The board is also very knowledgeable on other matters such as tax filing, payments, and adopts a holistic risk management approach.

We asked questions about product risk particularly as the company continues to evolve and innovate. In particular, we enquired about the impact of Quickbook and Credit Karma on its cyber risk. The company confirmed that all acquisitions are Intuit's employees and therefore they apply the same level of controls, access and security applied to laptops and training. At Credit Karma, the company is externally supervised to support alignment with the rest of the business. To further minimise the risk of an internal breach, every employee has access only to the data they need at the time.

We discussed the inclusion of cyber risk as an executive compensation KPI and the company requested more details of peers' best practice for its consideration. We provided an example of another company in scope. While we are satisfied with the company's use of simulations and tabletop exercises, the board has limited involvement in these practices but remain informed of progress. Concerning the company's reliance on cloud environments, it feels that as Amazon Web Services (AWS) invests enormous amounts in its own security, this relationship constitutes a benefit rather than a risk. This dynamic has been reiterated by other companies we have engaged with.

Best practice:

The company's audit and risk committee charter explicitly refers to cybersecurity as a significant risk.

Intuit plans to expand ISO 27001 to the whole business over time.

The company is a member of the Cybersecurity Tech Accord which emphasises user protection, partnerships and opposes cyber-attacks on innocent citizens and enterprises. The company also has a responsible disclosure programme that welcomes external input from communities. This works well, when issues are found, they duplicate them and fix them. Intuit is also a user of HackerOne.

NatWest

Engagement Type: Meeting

Outcome: Positive

Details:

We met with NatWest's Chair of the Board and Group Chief Administrative Officer. The board risk committee has ultimate responsibility for cybersecurity risk. The board has received frequent risk reports (including cyber) during the pandemic, with a slight decline with reports now on a monthly and quarterly basis.

The company spoke candidly and at length about the Travelex and SolarWinds large scale attacks that occurred in 2020. While the company feels it has made progress in building its resilience, it does not consider cyber risk to be a stagnant issue as the nature of the threat evolves over time. With regards to the Travelex situation specifically, it was not considered "catastrophic", but while it did not compromise the network, the level of misalignment resulted in the company rescinding the relationship until it could re-establish its capabilities. This move could be inconvenient for customers but NatWest expressed its discomfort maintaining the relationship. Executives and the board at NatWest are subject to continuous professional development, which includes ESG areas such as climate and cybersecurity risk.

Orpea

Engagement Type: Meeting

Outcome: Positive

Details:

We met with a very relevant set of representatives including Orpea's Head of Audit and Risk (reporting to CEO and VP Secretary General, both of which are regularly debriefed on audit issues), its Chief Information Security Officer (CISO), and investor relations staff. Lack of details about board oversight over cyber risk is compensated by a detailed description of systems for mitigation. There is particular emphasis placed on the risk to data security (sensitive medical records) and the enhanced risk experienced during the pandemic. Board oversight, internal controls, systems, and teams were provided during the meeting with the company. It was notable that the company does not evaluate net risk but rather assesses the gross risk faced, with a separate assessment of its management. This way, the board and top leadership remain aware of the risk significance. The company also shows a clear delineation and yet collaboration between internal audit and risk management.

The company demonstrates its focus on cybersecurity through innovation and systems evolution. In addition, Orpea adopts both a global and localised approach to the management of cyber risk. This considers their employees, systems and M&A activity.

London Stock Exchange Group

Engagement Type: Meeting

Outcome: Positive (best practice)

Details:

The extent and quality of disclosure by the London Stock Exchange Group (LSEG) is commendable. We praised the company for this, highlighting the multiple areas of best practice we observed. LSEG clearly identifies key roles such as executive leads, Chief Information Officer and Chief Information Security Officer (CISO) publicly on its website.

The company is heavily reliant on technology and as such has identified cybersecurity, resilience, and operational excellence as "fundamental parts" of its strategy. This is also a consequence of the company's migration of operations to cloud computing. The company includes information and cyber security threats among principal risks that fall under its operational risks, particularly the danger of conflicting or duplicative regulatory requirements.

During our meeting with the company's CISO, we were provided with more details on how the group is integrating Refinitiv and its technologies into a seamless group process following its merger. In its annual report, the company indicated that it engaged with regulators on cyber and technology preparedness — we seized the opportunity to request more details of these interactions. LSEG confirmed this referred to engagement with the Bank of England and regulators that oversee its operations on an ongoing basis to strike the right balance between the high levels of scrutiny and the best levels of disclosure.

The company provides details on the training schedule and the frequency of risk reviews in its annual report.

During the meeting we queried the lack of disclosure on breaches or near misses and whether this was an accurate reflection of the number of reportable cases. The company confirmed that it is transparent and that the one case the media confused for a cyber-attack, was later dispelled as an outage on main markets and was happy to provide details.

Best practice:

The remuneration report includes details of the group bonus pool and strategic deliverables which refers to the cybersecurity programme and the cyber & information risk operating model across the "three lines of defence".

The company includes a description of its enhanced cyber security systems in its Opex analysis.

Best practice:

ISO 27001 supports the relationship with suppliers and value chain, including unscheduled audits and the requirement to include cybersecurity clauses in contracts and health data host (HDS) certification.

The cyber risk management section of the company's annual report is very detailed, inclusive of case studies and specific actions taken to mitigate risk. Also included are metrics and further actions for risk mitigation.

We felt there was sufficient disclosure of incidents accompanied by detailed descriptions of all steps followed. Our discussions with the company indicated a no-blame culture with a focus on problem solving.

Progressive

Engagement Type: Meeting with follow up exchange via email

Outcome: Positive

Details:

We were able to cover our cybersecurity concerns during a financial update with the company. Otherwise, the company clarified they did not have records of having received our letter requesting a meeting.

During 2020, given the increased exposure as a result of having the entire workforce working from home, Progressive enhanced its cybersecurity risk management and created a technology committee at the board level. Prior to this, cyber risk was managed under the company's audit committee. The company is enhancing its disclosure, looking at MSCI, Sustainalytics and S&P methodologies to address these frameworks' main concerns. The company mentioned that their new sustainability report would be ready by summer and would include significant enhancements on this issue. It has not had any significant incidents to report and are obliged in California and other states to report cyberattacks and near misses. Representatives explained that the extensive regulatory oversight can be taxing.

They agreed to us forwarding detailed questions to address their risk management practices and when we followed up to request additional information, we were pointed to the enhanced disclosures on cybersecurity within their 2020 CSR report (published July 2021).

The report indicates that as an insurance company that heavily leverages client data, data protection is a core focus. The company provides clear disclosure on governance of cybersecurity risks. In 2020 Progressive created a new board technology committee with oversight of Cybersecurity, partly in response to the increased shift to digital due to the pandemic. The board committee director skills disclosures include cybersecurity.

The management structure in charge of monitoring the risk is described with the joint work of the Chief Security Officer and Chief Technology Officer. They report at least 5 times a year to the board on cybersecurity risk and management strategy. The company cybersecurity policies are part of General Business Principles and use ISO27002 to guide their cybersecurity policy. The CSR report briefly mentions training and education to their staff.

Progressive do not disclose and were not able to respond to our questions regarding metrics to measure their resilience, engagement with outside experts, simulations or 'lessons learnt' from previous attacks.

Best practice:

The company clearly articulates cybersecurity risk as a supplier risk category they monitor. They incorporate cybersecurity risk in how they monitor their suppliers and clearly reference how they review suppliers with regards to: "exposure to services or goods with potential cybersecurity vulnerabilities (inherent) or a lack of supplier cybersecurity controls (residual)".

TotalEnergies

Engagement Type: Meeting

Outcome: Positive

Details:

We met twice with TotalEnergies at our request. We found the initial conversation held with its investor relations department underwhelming, as it did not provide us with the necessary details and comfort needed that the risk was being actively mitigated. This was particularly important in light of the company's diversification into other business lines, namely electricity as part of its energy transition.

During our first meeting, the conversation, while generous in time and openness, did not cover all our concerns. The representatives from the investor relations and ESG team kindly offered a second meeting for us to discuss our cyber concerns with the subject matter experts.

A particular area of concern was that TotalEnergies, like many of its European peers, has taken a diversification route into electricity in order to achieve decarbonisation. In our experience, companies in the electricity utilities seem to have much more advanced procedures, systems and awareness of cyber risk.

A reassuring point is that the current CEO is also a board member of CapGemini and as such is acutely aware of risks resulting from information technology. We noted that he was also in charge of E&P Financial Group's information systems 15 years ago.

During our second meeting we met the company's Chief

Information Security Officer (CISO) who proved to be a very robust leader and deeply connected with the board.

We found that the CISO made use of good internal risk management practices, which mimic methods used in the defence service. Under their leadership, the company adopts a very credible (and aggressive) approach to supply chain risk.

There is a heightened focus on prevention and detection at the company, and a zero-tolerance approach to ransom.

Best practice:

A demonstrable approach is taken for third-party cyber risk by the firm. Its no compromise policy dissolves the relationship with third parties at the first sign of suspicion.

TSB Bank (part of Banco de Sabadell)

Engagement Type: Meeting

Outcome: Positive

Details:

We had a detailed dialogue with representatives of both Banco Sabadell and TSB Bank, from Spain and the UK. The focus of our discussion was the evaluation of how the group's detailed processes is applied to its operations in the UK. The general feeling was that while TSB had a long-standing brand, under Sabadell it is a better digital bank. The company confirmed that the technology used at TSB was enabled by Sabadell but is now based in the UK. It is linked with the Group but is run separately. Sabadell's modern infrastructure is an advantage for TSB against competitors that run on legacy systems.

The company confirmed that staff-wide cyber training is mandatory and occurs annually. At board level the company feels that they have sufficient levels of expertise. The board has regular briefing sessions and deep dives to understand the subject further.

The company has a suite of external advisors including IBM, Microsoft and KPMG, EY, BT and Deloitte.

In general, we found a very comprehensive description of the systems used in Sabadell's ARA, inclusive of metrics, and processes to minimise cyber risk.

Philips

Engagement Type: Letter exchange (following an ESG meeting)

Outcome: Positive

Details:

We had a dialogue on various ESG issues that did not afford us sufficient time to discuss our interest in cybersecurity. As a follow up meeting was proving difficult to schedule we requested the company to provide additional detail on targeted questions from our desk-based research.

Our analysis of the company's disclosures shows the existence of a Security Steering Committee and Group Security function; however, we requested more information about Director responsibilities and how the Board acquires and refreshes its knowledge on cybersecurity.

The company has very advanced cybersecurity mechanisms for its healthcare segment (e.g., Cybersafe) and we asked how this applied to the other business lines (e.g., personal goods). We also requested more details about the company cybersecurity culture and use of external experts. The company confirmed there is constant company-wide security communications related to potential threats and necessary actions to be taken. There are various mandatory trainings (and simulations) which are tracked and reported on under the governance described above. Furthermore, there is a continuous global phishing mechanism running to educate users to spot these risks. And there is an annual global security event in October to highlight important topics.

The company confirmed that its global security policies are approved at board level and are part of general business principles and subject to disciplinary measures. There is also a functioning global crisis management process, which covers cyber related incidents for which there is a dedicated process.

With regard to the use of external experts and assessments, the company confirmed the use of ISO27x, HiTrust, SOC2, depending on the area. The company also confirmed they work intensely with their suppliers to enhance security and have strict agreements on quality of security delivery and services.

With regard to transparency regarding major cyber threats and near-misses, the company confirmed they had not had any major security events in the past years and that their policy on disclosure is sent to the Security Steering Committee and Audit Committee as well as the company's external auditor. The company assess internally on a case-by-case basis cyber related incidents and whether the impact to its key processes and/or external presence is of a severity and/or financial level that needs external disclosure.

Best practice:

The company publishes security advisories[5].

5 philips.com/a-w/security/security-advisories

Conclusions and recommendations

Of the 37 companies in scope for this project to date, only one, H&M, openly rejected our offer to discuss their cybersecurity activities during both phases of the project. While we made a second attempt to open a dialogue in phase 2, due to the small size of our holding, we have decided not to pursue another avenue to escalate our engagement.

As we reported during phase 1, due to the sensitive nature of cybersecurity disclosures, most companies have only partial cybersecurity information published on their websites. We have reinforced our understanding of the companies' practices towards cyber resilience and the importance of the inclusion of an executive (e.g., CISO) or board member with responsibility for information security and cyber-resilience. However, this is no proxy for robust systems, training and most importantly, a cyber-resilient corporate culture.

During phase 2, we made an effort to evaluate any residual vulnerabilities through third parties. The most robust systems include direct communication of expectations to third parties, inclusion of covenants in contracts, vulnerability tests, continuous monitoring (with emphasis on critical relationships and functions), and effective exits for breaches of contract terms. We have also identified vulnerabilities during the integration of new business after a merger or acquisition and were more explicit in asking about this during our meetings.

As a result of the benefits gained from direct discussion with companies during phase 1, we initiated phase 2 of our cybersecurity engagement project with the intention of unearthing further best practice and escalating our activity to phase 3. However, our completion of phase 2 provides us with additional evidence to revisit our expectations. In the place of a full, public cybersecurity policy, we would seek the following minimum expectations that demonstrate effective management of cybersecurity risk:

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 cybersecurity 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 Cybersecurity Framework as a reference for cybersecurity risk management.
- ISO 27000 for all operations.
- Evaluation of cybersecurity in board effectiveness review.

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.co.uk

Ref: PDF RLAM PD 0062