PRI Principles for Responsible Investment

ENGAGING ON CYBER SECURITY: RESULTS OF THE PRI COLLABORATIVE ENGAGEMENT

2017- 2019

UNEP FINANCE INITIATIVE | United Nations Global Compact

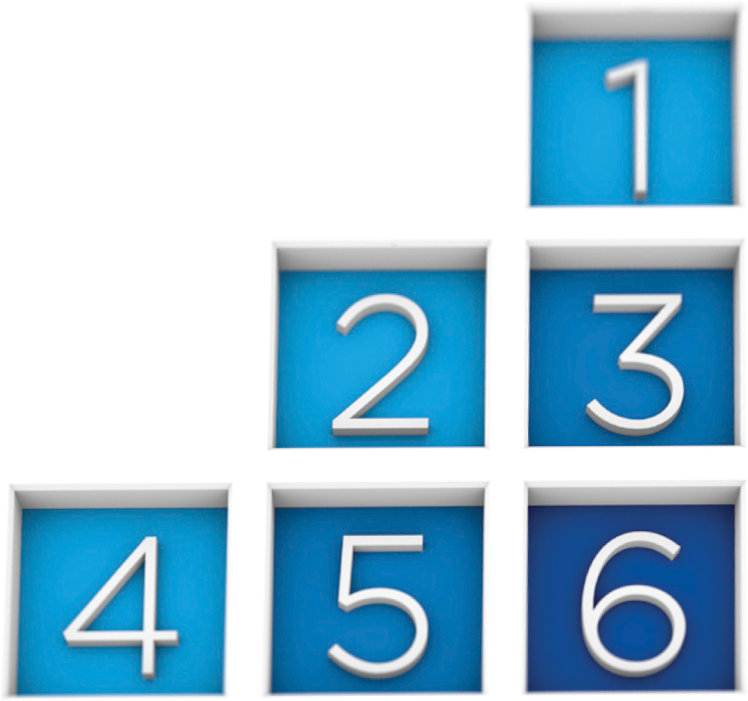
An investor initiative in partnership with UNEP Finance Initiative and UN Global Compact

THE SIX PRINCIPLES

PREAMBLE TO THE PRINCIPLES

As institutional investors, we have a duty to act in the best long-term interests of our beneficiaries. In this fiduciary role, we believe that environmental, social, and governance (ESG) issues can affect the performance of investment portfolios (to varying degrees across companies, sectors, regions, asset classes and through time). We also recognise that applying these Principles may better align investors with broader objectives of society. Therefore, where consistent with our fiduciary responsibilities, we commit to the following:

1. We will incorporate ESG issues into investment analysis and decision-making processes.
2. We will be active owners and incorporate ESG issues into our ownership policies and practices.
3. We will seek appropriate disclosure on ESG issues by the entities in which we invest.
4. We will promote acceptance and implementation of the Principles within the investment industry.
5. We will work together to enhance our effectiveness in implementing the Principles.
6. We will each report on our activities and progress towards implementing the Principles.



PRI's MISSION

We believe that an economically efficient, sustainable global financial system is a necessity for long-term value creation. Such a system will reward long-term, responsible investment and benefit the environment and society as a whole.

The PRI will work to achieve this sustainable global financial system by encouraging adoption of the Principles and collaboration on their implementation; by fostering good governance, integrity and accountability; and by addressing obstacles to a sustainable financial system that lie within market practices, structures and regulation.

CONTENTS

ACKNOWLEDGEMENTS

We would like to thank the following advisory committee members for their contribution to the project:

- Felipe Gordillo, BNP Paribas Investment Partners
- Mike Lombardo, previously at Calvert Investments
- Dominic Burke, previously at Hermes Fund Managers
- David Patt, previously at Legal & General Investment Management
- David Sheasby, Martin Currie Investment Management
- Rosa Van Den Beemt, previously at NEI Investments
- Chris Anker, previously at Railways Pension Trustee Company
- Melanie Adams, RBC Global Asset Management
- Claire Veuthey, previously at Wells Fargo Asset Management

The investors that participated in this collaborative engagement include:

- Aberdeen Standard Investment
- Acadian Asset Management
- AGF Investments Inc
- AMP Capital Investors
- Amundi
- Angel Oak Capital
- Australian Ethical Investment Ltd
- AustralianSuper
- Aviva Investors
- Bank J Safra Sarasin Ltd
- Bell Asset Management
- British Columbia Investment Management Corporation
- BlueBay Asset Management
- BMO Global Asset Management
- BNP Paribas Asset Management
- Caisse de dépôt et placement du Québec (CDPQ)
- Calvert Research and Management
- Candriam Investors Group
- Cometa Pension Fund
- Comgest
- Core Capital Management LLC
- EdenTree Investment Management Ltd
- FnB Private Equity
- GAM Investments
- Groupama Asset Management
- Handelsbanken Asset Management
- Federated Hermes
- Insight Investment
- Jarislowsky Fraser Limited
- Kempen Capital Managament NV
- Lancashire County Pension Fund
- Legal & General Investment Management (Holdings)
- LGPS Central Limited
- Liontrust / Alliance Trust
- Local Authority Pension Fund Forum
- London Pensions Fund Authority
- Manulife Asset Managemnt
- Maple-Brown Abbott Limited
- Martin Currie Investment Management
- NEI Investments
- Neuberger Berman Group LLC
- NN Investment Partners
- NorthEdge Capital LLP
- Oldfield Partners LLP
- Rathbones Brothers Plc
- Railways Pension Trustee Company Limited
- RBC Global Asset Management
- Robeco
- Royal London Asset Management
- Sarasin & Partners LLP
- Sparinvest Group
- Sumitomo Mitsui Trust Bank, Limited
- Union Asset Management Holding AG
- Universities Superannuation Scheme
- West Midlands Pension Fund

EXECUTIVE SUMMARY

Cyber security has been recognised as a risk in the World Economic Forum Global Risks Report for several years, with the latest version ranking cyber security as one of the top 10 risks that the world will face in the next 10 years.[1] As the incidence of cyber attacks and the costs of security failures increase, institutional investors want to be on the front foot in assessing portfolio exposure to cyber security-related risks. However, poor corporate disclosure on this topic and lack of advanced technical expertise make it difficult for investors to understand how companies are addressing this growing challenge.

Against this backdrop, the PRI initiated a collaborative engagement with 55 institutional investors representing over US$12trn in assets under management. Using cyber governance as a proxy for cyber resilience, these investors engaged 53 companies in a range of sectors (healthcare, financial, consumer goods, information technology and telecommunications) over 2017-2019. On the basis of research commissioned by the PRI, they pressed for improved disclosure on cyber security policy, board oversight and reporting, access to expertise, training and assessment.

This report provides investors with:

- An analysis of how companies within this initiative have progressed on corporate reporting over the last two years;
- Insights from the PRI collaborative engagement that shed light on how cyber risks are being perceived and addressed among companies from diverse sectors; and
- A set of investor recommendations on engagement, including tools to benchmark disclosure and set expectations.

Over the engagement period, the targeted companies made significant strides in reporting on cyber-related governance mechanisms and processes. The average score across the companies improved from 6.1 to 8.5 (out of 14 indicators) over 2017-19. The number of companies leading on disclosure increased, as did the level of detail and scope of information disclosed. However, despite these positive trends, cyber security-related disclosures cannot be considered the norm – for instance, in 2019, a majority of the targeted companies did not provide information on audits, evidence of cyber security training for all staff or details of relevant board expertise.[2]

Nonetheless, companies were open and willing to engage in private conversations with investors and made their experts available to provide a comprehensive view of their approach to cyber security. The engagement conversations enabled investors to scrutinise governance practices and discuss current and future expectations around cyber security maturity. Key learnings from the dialogues regarding board oversight, board expertise, cyber security monitoring across the value chain and capacity building are explored in detail in the report.

The report also includes recommendations, potential engagement questions and disclosure expectations for investors looking to initiate or continue engagement on cyber security. At a high level, we recommend that investors:

- Validate board oversight of cyber risk;
- Ensure cyber resilience is integrated into corporate strategy;
- Check for common language;
- Look beyond technical controls; and
- Set disclosure expectations.

Furthermore, investors can use the set of disclosure expectations to identify gaps in company disclosure, benchmark portfolio companies against their peers, and as a tool for engagement to drive better disclosure on cyber security.

Going forward, and building on our work on cyber security, the PRI will explore related themes such as artificial intelligence and the ethics of innovation as well as appropriate governance mechanisms and regulatory gaps. To support investors in understanding related risks and opportunities and formulating their response, the PRI will also consider the broader implications of technology for sustainable development and responsible investment, looking across the entire investment chain.

1 World Economic Forum (2020), The Global Risks Report 2020.

2 See infographic on pg. 10.

INTRODUCTION

The proliferation of digital technologies has considerably increased the vulnerability of companies and governments to cyber attacks in recent years. A 2019 report from Accenture found that cyber security breaches had risen by over 65% over the last five years.[3] As increased automation and smart technologies are embraced, cyber threats are expected to become more frequent and intense. As a result, it is estimated that the cost of data breaches will rise from US$3trn each year to over US$5trn in 2024.[4]

The impacts are, however, not purely financial. The harms caused by cyber attacks can be reputational (e.g. damaged relationships with customers, intense media scrutiny and loss of key staff), societal (e.g. disruption to daily life through impacts on key services, a negative perception of technology), physical (e.g. loss of life, damage to infrastructure) and psychological (e.g. victims left depressed, embarrassed, shamed or confused).[5]

It is only prudent, then, that companies take measures to secure against a possible threat. However, this is easier than done given the increasing sophistication of attacks, inconspicuous nature of the instigators of cyber attacks and rising costs of cyber defence. In fact, several market studies have illustrated that companies are struggling with cyber risk management.[6] And corporate disclosures related to these practices fail to offer assurances to the contrary.[7]

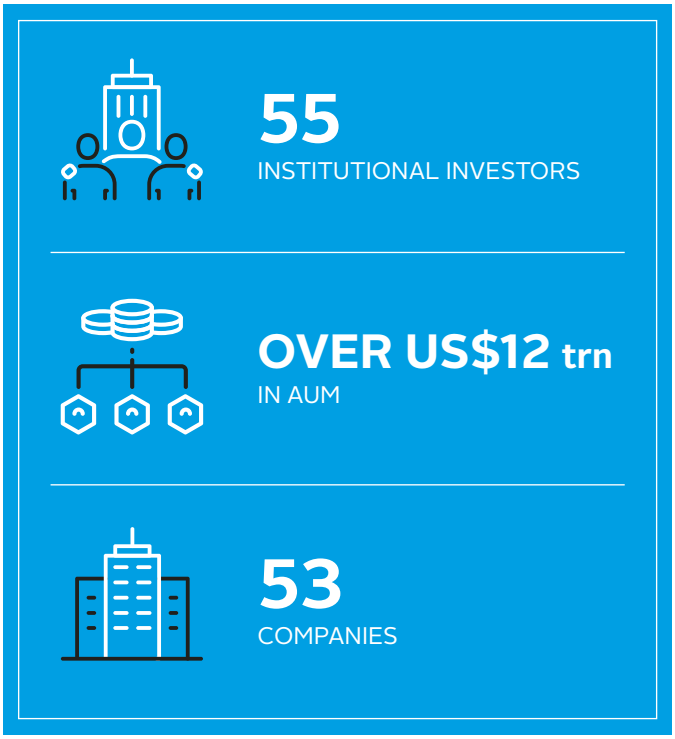
These cyber-related business challenges are, therefore, raising concerns for institutional investors. They are keen to develop better understanding of the scope of these risks and their potential impact on portfolio companies. However, the ever-changing cyber security landscape is complex to navigate – there are no established standards or ways to compare the levels of cyber risk across different sectors or companies.[8] Also, investors are not privy to internal management discussions around cyber readiness or incident management and rely on company boards and management for their oversight, governance and disclosure of this enterprise risk.

In this context, cyber governance can be a proxy for the strength of cyber resilience within the firm, allowing investors to assess whether a company has an organisation-wide approach to cyber security, without having to delve into technical nitty-gritty. Disclosures around governance would provide assurance to investors of appropriate policies and controls, levels of accountability and strong board oversight to validate the adequacy and sufficiency of cyber security procedures.

3 Accenture (2019), The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study
4 Business Losses to Cybercrime Data Breaches to Exceed $5 trillion by 2024, 27 August 2019, Business Wire.
5 Researchers identify negative impacts of cyber attacks, 29 October 2019, University of Oxford news release
6 The rising strategic risks of cyberattacks, Tucker Bailey, Andrea Del Miglio, and Wolf Richter, May 2014, McKinsey Quarterly
7 PRI (2018), Stepping up governance on cyber security
8 RBC Global Asset Management (2019), Cyber security and privacy: A material concern for investors

ABOUT THE ENGAGEMENT

In this context, the PRI initiated in June 2017 a collaborative engagement on cyber security governance. The engagement received significant interest from signatories – 55 institutional investors, with assets under management of over US$12trn, joined the group.



The focus of the engagement was defined based on input from an advisory group of investors and industry experts. While acknowledging that no business is immune to cyber attacks, the engagement was narrowed down to the financial, healthcare, telecommunications, information technology and consumer discretionary sectors based on an assessment of exposure to cyber security risks, frequency and impact of incidents, and responses to these incidents. For instance, the financial industry was a focus because of its continued exposure to threats (a 2019 Accenture report estimated the annual average cost of cyber crime for companies in the banking sector to be US$18.37m), despite companies demonstrating greater cyber readiness relative to other sectors. The healthcare industry, on the other hand, was selected because of the potentially catastrophic impact from a possible breach and the low level of preparedness across the sector.

To understand the state of play and gaps in cyber security-related disclosures across these companies, the PRI commissioned benchmark research in 2017. The companies were assessed against 14 indicators of cyber governance and risk management (see Figure 1). A key finding of this research was that there were no minimum standards of regular public disclosure on cyber security practices at large cap-listed companies. While companies generally perceived cyber security as a key organisational risk, very few communicated that they have policies, governance structures and processes that were effective at tackling cyber threats. Overall, the research concluded that companies must be encouraged to expand public reporting to demonstrate sound monitoring and management of risks.

9 Accenture (2019), The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study

10 Further research insights are available in the PRI report Stepping up governance on cybersecurity (2018)

Figure 1: Research indicators

LEGAL COMPLIANCE

1. Does the company publicly commit to compliance with all relevant laws, including those related to cyber and data protection?

POLICY

2. Does the company publicly disclose a privacy or data protection policy, or both?
3. Does the policy explicitly cover its entire operations, including third parties?

SENIOR MANAGEMENT AND BOARD ACCOUNTABILITY

4. Does the company identify a named person at senior management or executive committee level with overall responsibility for information management and cyber security?
5. Is the board or a board committee responsible for cyber security issues?

BOARD COMMUNICATION

6. Does the company communicate cyber risks to the board (and how, by whom and how often)?
7. Does the board receive detailed information about the company's cyber or information security strategy? (If so, what information is received, and how is it assessed)?

SKILLS AND RESOURCES

8. Does the company disclose that it has a cyber or information security team or dedicated budget?
9. Does the company state that the board engages with relevant industry initiatives on cyber security or has access to internal or external expertise on cyber security?
10. Does the company actively seek such skills when appointing directors?

TRAINING

11. Does the company provide training on information or cyber security requirements to all employees?

ASSESSMENT

12. Does the company conduct audits of information or cyber security policies and systems?

PROCESSES AND PROCEDURES

13. Has the company established an incident management plan (including disaster recovery and business continuity)?
14. Has the company disclosed information or cyber security as a key part of its risk assessment/business continuity plan?

Taking these findings into consideration, investors held meetings with 53 companies in the financial (20), healthcare (15), consumer goods (nine), telecommunication (five) and information technology (four) sectors over the course of this engagement. The key objectives of the collective engagement are outlined below:

Build investors' knowledge of how their portfolio companies are positioned to manage cyber risk (with a focus on companies' policies and governance structures)

The engagement conversations were structured to enable investors to scrutinise policies and governance practices, raise questions around approaches to cyber risks, and discuss current and future expectations around cyber security maturity. The engagement also sought to identify good practices and a create a better understanding of how equipped company boards were for tackling cyber security-related challenges.

Improve the amount and quality of company disclosure on cyber risk and governance.

The benchmark research, which scored companies on 14 indicators (see Figure 1), was used as the basis for investor-company dialogue. Through the engagement, investors sought to raise these scores and improve the quality of the information being published. A comparative analysis of disclosure over 2017-19 tracked progress against this objective; this is illustrated in the next section of the report.

Establish investor expectations on what companies can and should disclose regarding cyber risk governance.

The last objective was to draw up a list of indicators for public cyber security disclosure that could form the basis of investors' expectations on this topic. This list (see Recommendations, pg. 19) is intended to facilitate further investor engagement on the issue and enable the development of appropriate governance norms on cyber security.

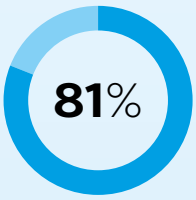
ENGAGEMENT PROCESS

2017	VS	2019
Average score (number of indicators met out of 14)		
6.1		8.5
Percentage and number of companies disclosing 10 or more indicators		
13% (seven companies)		42% (22 companies)
Percentage and number of companies disclosing two or fewer indicators		
21% (11 companies)		6% (three companies)

SECTOR SNAPSHOTS

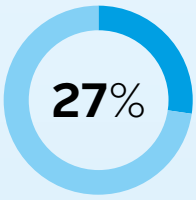
HEALTHCARE

AVERAGE SCORE (2019)	IMPROVEMENT IN DISCLOSURE
6.9/14	81%

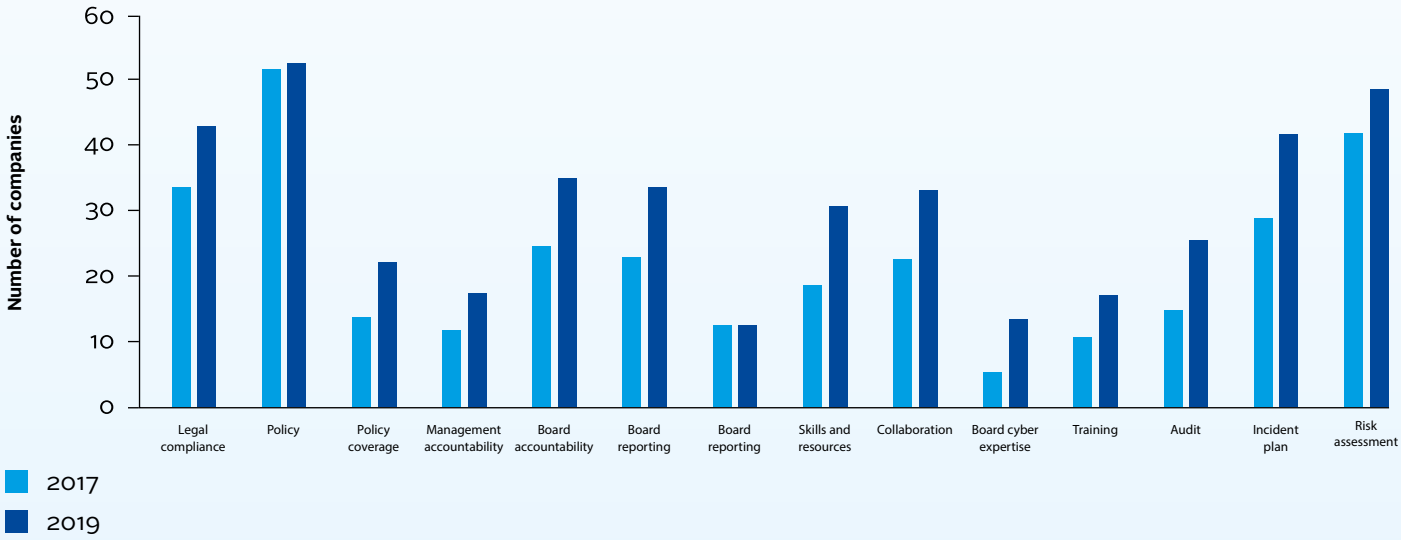


FINANCIALS

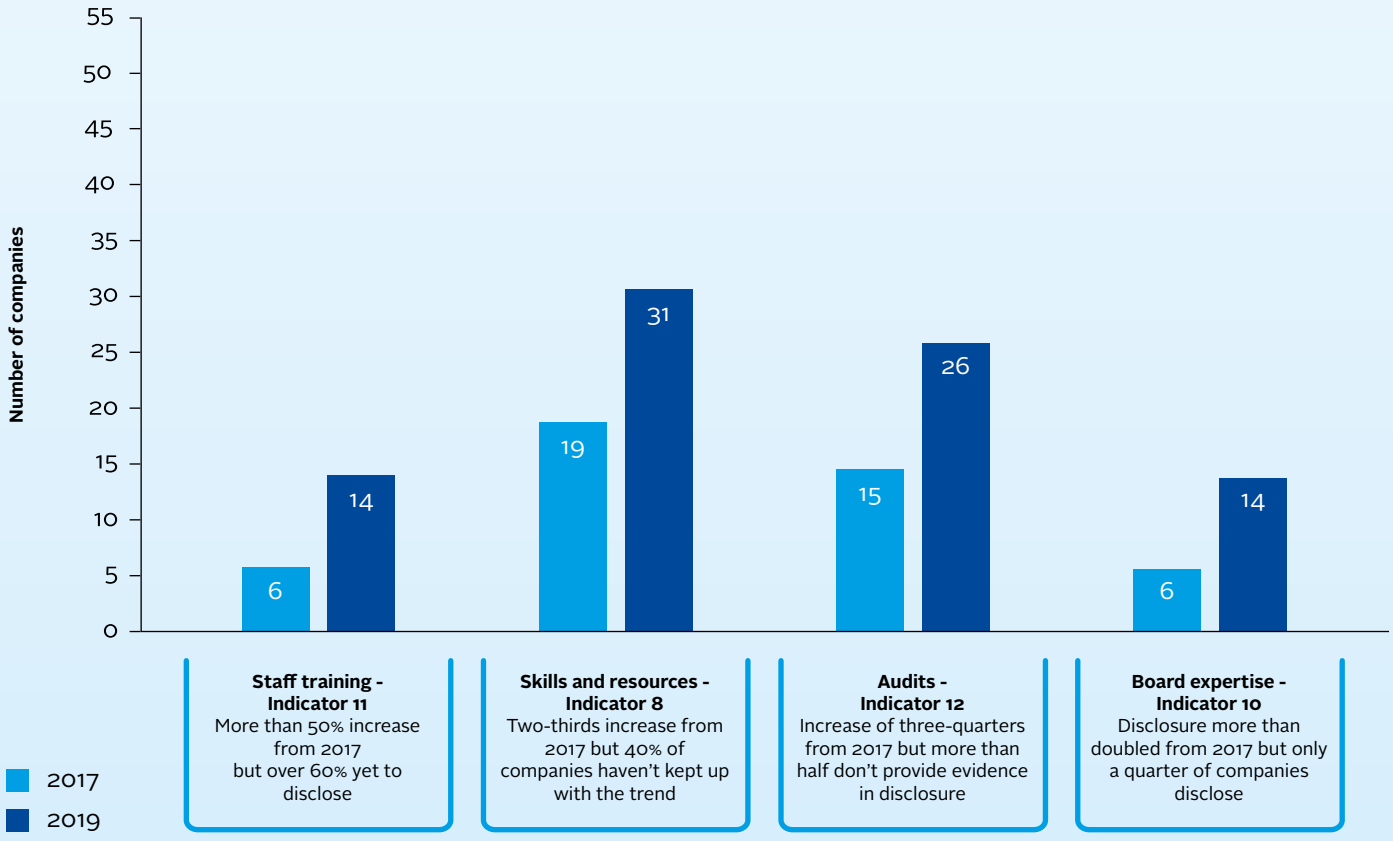
AVERAGE SCORE (2019)	IMPROVEMENT IN DISCLOSURE
9.8/14	27%



LEVEL OF DISCLOSURE ON RESEARCH INDICATORS



HIGHLIGHTS



Staff training - Indicator 11
More than 50% increase from 2017 but over 60% yet to disclose

Skills and resources - Indicator 8
Two-thirds increase from 2017 but 40% of companies haven't kept up with the trend

Audits - Indicator 12
Increase of three-quarters from 2017 but more than half don't provide evidence in disclosure

Board expertise - Indicator 10
Disclosure more than doubled from 2017 but only a quarter of companies disclose

ENGAGEMENT CASE STUDY: PROGRESS IN DISCLOSURE

Verizon Communications provides annual perspectives to businesses on what cyber threats they are likely to face in the coming year through its Data Breach Investigations Report. However, the PRI investor collaboration initially found very little public information on the company's own cyber security governance and management.

It was only through engagement, led by NEI Investments, with Verizon's General Counsel & Corporate Secretary and Chief Information Security Officer that it became clear that cyber security was a top enterprise risk for the company due to the sensitive nature of the customer data it handles and; that it had a number of best practice approaches in its operations and governance. These included board committee oversight of cyber security risk and product privacy, executive staff responsible for cyber security and privacy, the existence of a security council comprised of various department heads, and robust employee training on the subject.

The engagement encouraged Verizon to enhance its disclosure. The company also came under pressure from investors outside of the collaborative engagement to report on the feasibility of tying executive compensation to data security performance.

Following the engagement, Verizon significantly improved cyber governance disclosure in its proxy circular, transparency report and corporate responsibility reporting, meeting 12 of the 14 indicators (compared to 5 in the initial assessment) in PRI's assessment.

ENGAGEMENT CASE STUDY: FROM LAGGARD TO LEADER

Private equity firm Eurazeo demonstrated the greatest improvement as a result of the collaborative engagement on cyber security. The company's score increased from zero to 12 in PRI's assessments on cyber disclosure over 2017-19.

In the initial discussions Sparinvest, the lead investor for this engagement, learnt that Eurazeo was reluctant to publish the details of cyber security measures that were already in place. However, during the course of the engagement, the company reported that it had introduced a cyber security policy, set up a related governance framework and had conducted a risk materiality analysis on cyber security. It also began to disclose details on cyber training and insurance.

Sparinvest found that benchmarking the company against best-in-class peers and, specifically, discussing how other firms report on cyber security may have helped the company overcome initial concerns around reporting.

Sparinvest also found that cyber security is now part of Eurazeo's overall ESG policy towards its portfolio companies – meaning that the companies in which Eurazeo invests also benefit from its improved expertise in this field.

As a lead investor on the engagement with Eurazeo, Sparinvest noted: "We gained increased knowledge of the cyber security risks faced by companies in certain sectors and the policies that should ideally be in place to mitigate them. It has given us a useful framework for conducting investment analysis and future engagements with companies on this topic."

CYBER SECURITY IN PRACTICE: INSIGHTS FROM THE ENGAGEMENT DIALOGUE

The dialogues showed that cyber security continues to be a sensitive issue for corporates to talk publicly about. Some are concerned that too much disclosure may draw undesired scrutiny from hackers, while others are at early stages in terms of building an understanding of the issue, and therefore are not prepared to put detailed information in the public domain. These concerns may explain why there are still gaps in cyber security-related disclosures.

Nonetheless, in contrast to their initially limited public reporting, companies contacted through this engagement were open to private dialogue and willingly made their experts – usually chief information security officers or digital directors (as well as staff from their sustainability and investor relations teams) – available to help investors develop a more comprehensive view of how they are addressing cyber security risks. The level of access and the depth of information provided was extremely valuable for investors, who typically found it challenging to ascertain companies' positions from public disclosure alone.

The section below features key trends and investors' learnings from the engagement dialogue over 2017-19. It also outlines good practice examples on the following four areas:

I. Board oversight;
II. Board expertise;
III. Monitoring across the value chain; and
IV. Building capacity.

I. BOARD OVERSIGHT

BACKGROUND

To demonstrate that cyber security is an organisational priority, companies should establish board oversight of the issue. Boards have a role in ensuring that cyber security considerations are not just integrated into risk management, but that they also drive strategy and shape broader business decision making.[11] To enable this, board members should receive quality management information and be well-informed so that they can sense-check the adequacy of cyber security programmes, and challenge management actions where appropriate. This does not mean that the board should be involved in the day-to-day technical and operational issues. However, it must set expectations and have confidence that operational, financial and strategic resilience tied to cyber security is in line with those expectations.

DISCLOSURE

Gauging from public disclosure among the companies engaged during this process, board oversight of cyber security issues was far more common in 2019 than in 2017. Most companies engaged had allocated responsibility for cyber security at the board level – often via the audit committee, risk committee or a sub-committee of the risk committee focused on IT resilience (Indicator 5). In some cases, cyber security had been prioritised to the extent that a separate board committee was set up to provide strategic guidance and governance. This was more common among companies with more advanced thinking on cyber security.

> UK-based financial services company Standard Chartered disclosed that its financial crime risk board committee is composed of independent non-executive directors and external advisors with extensive experience in cyber security and international security; it said that the committee provides the company with "a valuable external perspective".[12]

11 Marsh (2018), Governing Cyber Risk: A Guide for Company Boards

12 Standard Chartered, Annual Report 2018, p. 89

Several companies also indicated that their board or the board sub-committee received frequent updates, usually half yearly (if not quarterly) from the chief information and security officer (CISO), the chief information officer (CIO), or executive committees with cyber security-related responsibilities.

For instance, Australian financial group Suncorp Group, began to disclose in 2019 that its board is responsible for overseeing cyber security and that "cyber risks are reported at least quarterly through the Board's Risk Committee."[13]

However, companies lagged in their reporting of details of what information the board receives and how it is evaluated. While there were some improvements since 2017 (see example below), almost three-quarters of the engaged companies were yet to make progress on disclosure (Indicator 7).

Booking Holdings, a US-based engineering company, disclosed that its audit committee regularly reviews and discusses with management the company's exposure to cyber risks. The audit committee reports to the board quarterly on this topic, "including impact on operations, business and reputation, the steps management has taken to monitor and mitigate such exposures; [and] significant legislative and regulatory developments that could materially impact the company's privacy and data security risk exposure".[14]

ENGAGEMENT INSIGHTS

Given overall inadequate public disclosure, investors were keen to understand through the engagement how boards exercise oversight of cyber security matters. They raised questions around the extent and quality of reporting to the board and how this is evaluated and challenged to steer cyber resilience across the organisation. They found that this level of information was critical to develop a view around the robustness of decision making on cyber security issues within the firm. Some of the key themes are discussed below.

Board reporting

Most companies revealed that, at a minimum, their boards received briefings from senior executives to educate them on cyber risk exposure. These briefings usually cover details of the threat environment, key industry incidents and how peers are addressing cyber risk. Some companies went further, contextualising these updates and informing the board of appropriate policies, cyber security risks and the probability of their occurrence, and cyber defence enhancements.

Companies that are leading on cyber security made it clear that their boards were well ahead in terms of assessing impacts on the business and agreeing on a level of risk tolerance. Cyber risk was incorporated into enterprise risk management systems, as opposed to being considered in isolation; as a result, regular risk reports were prepared by the CISO for the board. Furthermore, board members at these companies did not rely on one-way updates but actively participated in discussions with senior management on progress against expectations and improvement plans. For instance, one British retailer stated that there had been in-depth discussions between a non-executive director and the head of technology relating to the cyber security plans of one of its divisions.

Key performance indicators

A few companies indicated that they are looking to develop (or are in the process of developing) appropriate measures of cyber security performance for internal reporting. While a small selection of companies expressed reservations about sharing this information with the investor group, others provided granular detail. One US-based telecoms company said that it tracks metrics at different levels within the organisation (staff, management and executive) and reported to the board committee.

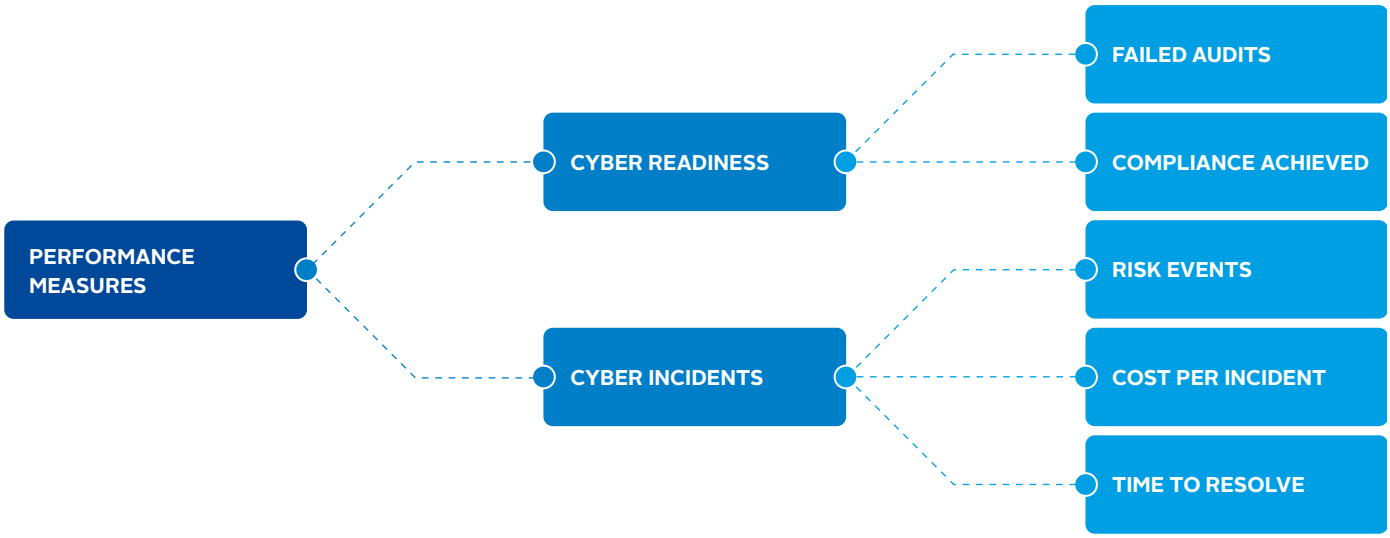
Overall, the performance measures and metrics that were highlighted in the dialogues can be grouped into two broad themes (see Figure 2):

- Cyber readiness, e.g. compliance scores, failed audits, data loss prevention and quantitative data on vulnerability management, security infrastructure and anti-malware; and
- Incidents, e.g. risk events, number of attacks, cost per incident, time to resolve etc.

13 Suncorp, Corporate Governance Statement 2017-2018, p. 19

14 Booking Holdings (2018), Audit Committee Charter, p. 5

Figure 2: Commonly identified measures of cyber security performance



Despite this level of communication, however, companies offered limited insight on how these metrics were selected or updated, and how they contributed to board evaluation of cyber security plans.

In a rare exception, a French financial institution provided investors with a deeper understanding of how metrics reported to the board add value to directors' assessment of vulnerabilities and led to subsequent strengthening of cyber security plans. It explained that its board had received detailed scores on cybersecurity maturity for each of its subsidiaries following an independent analysis in line with information security standard ISO27001.[15] This led to the company setting annual targets for cyber security improvements at each of its subsidiaries, which consequently led to improvements across the organisation.

Examples such as these highlight the role of board processes in relation to cyber security, in terms of evaluating current plans and driving strategic changes across the company. While investors may not have a pre-determined list of cyber security KPIs that companies should use, they certainly want board reporting to be useful, forward looking and actionable. Large volumes of retrospective cyber attack information are unlikely to promote informed decision-making within the company.[16]

Escalation and incident reporting

Many companies admitted to investors that they deal with cyber attacks on a daily basis. Some said they had been subject to denial of service attacks which aimed to shut down their networks and disrupt business by cutting off access to customers. While it was clear that these companies were actively reporting to the board on the number of cyber breach incidents and their impact, the conversations often did not describe escalation mechanisms and the type of incidents that triggered reporting.

In conclusion, companies signalled different levels of comfort in effectively communicating cyber security matters internally and externally. While practices varied, they nevertheless provide an indication of the strength of cyber security governance. Seeing examples of good practice assured investors that the absence of reporting does not necessarily signify lax attitudes to proper governance arrangements.

15 ISO27001 is an international standard for information security management systems, a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes. Its technical definition can be found here.

16 TheCityUK (2018), Governing cyber risk: a guide for company boards

II. BOARD EXPERTISE

BACKGROUND

There has been some debate around whether board members should have cyber security expertise akin to qualified financial expertise. Some experts believe that, given the importance of technology in the modern economy and the prevalence of cyber risk, it is crucial that boards have specialist skills in this area. A recent MIT study found that companies with "digital savvy" boards tended to achieve greater revenue growth, return on assets, and growth in market capitalisation compared with their peers whose boards lacked such skills.[17] Other experts think that cyber security is just one of many issues that boards need to evaluate, and therefore does not justify particular proficiency. They believe senior management is best placed to handle cyber security on a day-to-day basis, as long as the board is kept aware of the significance of the risks faced and how they are being managed.[18]

DISCLOSURE

Over the course of the last two years, a growing number of companies in the engagement demonstrated that they were addressing board expertise on cyber security. Some companies reported that cyber security skills were explicitly considered when recruiting new board members (Indicator 10).

> For example, Dutch financial company ING Group said that information technology is one of the areas of competence that is considered in the composition of its supervisory board, which is responsible for supervising and advising the executive board on cybersecurity risk.[19]

However, such details were provided by only 14 of the 53 companies engaged. Even among companies that had board members with relevant expertise, it wasn't clear if such expertise was the decisive reason for appointing that member.

ENGAGEMENT INSIGHTS

Given that this was one of the least disclosed indicators, despite increased calls for cyber expertise on the board,[20] investors were keen to understand companies' perspectives on the issue.

In the engagement dialogues, most companies did not rule out the possibility of appointing directors with cyber security specific skills. However, they did not flag this as a priority criterion for board appointments. Companies said they were looking for a spectrum of relevant experience, and while cyber and IT skills are included in the mix, they could not be considered in isolation but in the context of existing and desired board composition.

The conversations also revealed that many companies were prioritising training to address deficits in board knowledge and expertise. For instance, a Dutch financial company told investors that it trained its management and supervisory boards twice a year, covering reports on the cyber-threat landscape i.e. what attacks look like and how they are evolving. Other companies indicated that they conduct board exercises to ensure their boards have the necessary guidance to respond to a major incident in terms of communication to the press, customers, regulators etc.

In addition to training, companies also look to external advisors to upskill their boards, facilitate strategic discussion and ensure that board members are able to ask the right questions and challenge senior management on cyber security. To this end, several companies said they had set up independent advisory panels and retained specialist consultants.

Overall, the engagement dialogues showed that companies have nuanced positions on board expertise on cyber and looked to training and external expertise where skill gaps were found – something that disclosure alone did not reveal.

17 It Pays to Have a Digitally Savvy Board, Peter Weil, Thomas Apel, Stephanie L. Woerner and Jennifer S. Banner, 12 March 2019, MIT Sloan Management Review

18 See, for example, Council of Institutional Investors (2016), Prioritizing Cybersecurity: Five Investor Questions for Portfolio Company Boards.

19 ING, Supervisory Board Charter and Profile, as of 31 December 2019

20 See, for example, Good Governance: Do Boards Need Cyber Security Experts?, Robin Ferracone, 9 July 2019, Forbes.

III. CYBER SECURITY MONITORING ACROSS THE VALUE CHAIN

BACKGROUND

Companies are increasingly reliant on the collection and processing of private data in their everyday business activities. Many use third parties and partners for these services. However, there are concerns that associates in the value chain, including suppliers and vendors, are weak links when it comes to a cyber security: they hold or have access to sensitive data but may not have appropriate policies and processes in place to adequately protect it. This creates pressure on companies to be proactive in setting high standards and identifying weak security measures in their value chains in a timely manner.

DISCLOSURE

If disclosures are considered a reflection of cyber security practice, companies may not be doing enough. Even at the policy level, as of 2019 only 60% of engaged companies were yet to provide evidence of extension of their data protection and privacy policies to global operations and third parties (Indicator 3). This is concerning, because threats that may cripple external providers are likely to cause reputational and financial damage across the value chain.[21]

One company that did provide evidence of appropriate policies in this context was Novo Nordisk.

> In its privacy policy, the Danish pharmaceutical company not only commits to be in compliance with personal data legislation, but states that it extends these standards to its value chain: "Although the legal obligations under European law apply only to personal information used and collected in Europe, Novo Nordisk will apply this Policy globally, and in all cases where Novo Nordisk processes personal information both manually and by automatic means, and whether the personal information relates to Novo Nordisk's employees, contractors, business contacts or other third parties.[22]

ENGAGEMENT INSIGHTS

The engagement dialogues found that some companies were waking up to the potential risks around third-party practices. For instance, a financial company confirmed that it experienced nearly double the volume of attacks in 2017 compared to the previous year and many were attacks that targeted its suppliers. As a result, the company was increasingly focused on supplier vulnerability. A large retailer said that it ranked third-party risks among the highest cyber exposures it faces and had begun a monitoring process for sub-contractors on a case-by-case basis.

Some companies also stressed that value chain risk is often an industry-wide issue, so they were devising plans to address these risks with peers. For example, one bank indicated that it meets with other financial institutions every week to share intelligence on cyber security challenges.

However, generally speaking, companies' efforts to address third-party risks appear to be piecemeal. A notable exception is a US-based medical device company, which has a sophisticated process for monitoring its value chain. It provided detailed information around monitoring of third parties, which includes systematic due diligence before signing contracts, ensuring secure boundary control for data, periodically reassessing partners' cyber security performance and requiring them to share the results of regular penetration tests. It also stated that partners engaged for medical research were vetted via a security and privacy assessment and, when concerns emerged, they were required to undertake remediation or incorporate binding obligations in the contract.

Overall, the engagement showed that there is much more for investors to do to drive systematic policies and processes within companies on third party-related cyber security risks.

21 For examples of recent high-profile incidents, see Verizon (2019), Data Breach Investigations Report.

22 Novo Nordisk (2019), Data Protection Binding Corporate Rules Policy

IV. BUILDING CAPACITY

BACKGROUND

A study of a representative sample of companies found that, on average, the annual cost of cyber crime per company reached US$13m in 2018, an increase of 72% over the previous five years.[23] This raises questions around how companies are strengthening organisational capacity, including through recruitment and allocating appropriate budget to cyber security products, services and training staff. Staff training is an important element of risk management, as insiders often represent the weakest link in terms of cybersecurity.[24]

DISCLOSURE

The answers to these questions are not always readily available in company reports. In fact, companies in the engagement raised concerns that such disclosure may attract unnecessary attention and testing by hackers. Nevertheless, the uneasiness to report may be declining, given the improvements in disclosure seen since our benchmark research in 2017 (with an increase from 19 to 31 companies reporting on Indicator 8).

An increasing number of companies have also started to disclose information around capacity building, detailing external expertise and collaboration (Indicator 9) with peers and national governments.

Some examples include:

Johnson & Johnson, a US-based healthcare company, which has an information security team which maintains "close working relationships with peer companies, industry associations and government agencies, both to share best practices and to collaborate on effective solutions to address the increasing threats and attack methods faced by both public- and private-sector organisations today".[25]

AXA, a French insurance firm, which set up in 2015 a data privacy advisory panel, composed of experts in data privacy, including academics, members of think thanks and former members of regulatory bodies. The advisory committee meets twice a year in Paris.[26]

BT Group, a British telecommunications company, which launched in 2018 a free collaborative online platform to share information about malicious software and websites with its peers to help prevent cyber crime.[27] This initiative is the result of collaboration with the National Cyber Security Centre – a UK government body that provides advice and support on computer security threats avoidance. BT believes that it is the first telecoms firm in the world to share this type of data with the industry.[28]

ENGAGEMENT INSIGHTS

During the engagement, investors sought to gain a better understanding of how corporate cyber security functions are resourced and equipped to defend against threats. Discussions found that companies had significantly increased their investments in this area in the last few years, increasing their capacity to deal with security issues and protect data. This is in line with industry research that suggests steep growth in corporate spending on cyber security products and services.[29]

The financial sector appears to be leading the way. For instance, one French financial firm quadrupled its cyber security spend over 2014-17 and increased the size of its team from 10 to hundreds over the period. This strategic shift was attributed to digitalisation, increasing criminality and terrorism, industry trends and internal assessments.

That said, companies are also strengthening capabilities and resilience through other ways – for instance, via the use of external service providers, providing training for staff, purchasing cyber security insurance, and collaborating with peers.

Companies indicated that they used external vendors and service providers to bring expertise to their teams and for testing and auditing purposes. At several companies, vendors conducted regular penetration tests to identify cyber vulnerabilities and work with internal specialists to remedy identified issues.

Some companies said that they were investing in their staff to mitigate risks. For instance, a British financial company indicated that it is making training more interactive through gamification – it said that 1,500 employees joined cyber games on a voluntary basis. The company is also working to build a culture of awareness by recruiting information security champions in every location. The champions are non-experts but are responsible for raising the importance and visibility of cyber risk.

23 Accenture (2019), The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study

24 See Accenture report above for examples.

25 Johnson & Johnson, Health for Humanity Report 2018, p. 103

26 AXA, Data Privacy Advisory Panel webpage.

27 BT, Digital Impact and Sustainability Report 2018/19, p. 17

28 NCSC, What we do webpage.

29 Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019, 15 August 2018, Gartner press release.

Certain healthcare companies spoke about the use of cyber security insurance to minimise cyber security-related losses and secure business operations. They were of the view that insurance forms part of a comprehensive cyber security strategy, even though it does not prevent a cyber attack or fully compensate a company after one occurs. Other companies, however, expressed reservations: given rising premium costs and confusion about what cyber insurance does and does not cover, they preferred to self-insure through dedicated provisions.

Some companies indicated participation in collaborations coordinated by national governments to promote higher standards and drive better behaviours to handle threats that may not be as well understood. One example is run by the US Food & Drug Administration (see Box, The FDA's Precertification Pilot).

THE FDA'S PRECERTIFICATION PILOT PROGRAM

Set up in July 2017 by the US Food & Drug Administration, an agency within the U.S. Department of Health and Human Services responsible for protecting public health, the Software Precertification Pilot Program focuses on improving safety standards of software technologies in medical devices.[30] Participants in the voluntary initiative include Apple, Fitbit, Johnson & Johnson, Pear Therapeutics, Phosphorus, Roche, Samsung, Tidepool and Verily.[31] The pilot is still ongoing, and a summary of the FDA's test activities was published in July 2019.

Another example is the Bank of England in the UK (see Box, Sector-wide simulations at the Bank of England) which has established a number of working groups to discuss sector-level challenges and consider third-party review processes.

SECTOR-WIDE SIMULATIONS AT THE BANK OF ENGLAND

The Bank of England Security and Operations Centre has set up an initiative to evaluate the operational resilience of the banking sector. As a part of this, it is conducting an annual simulation to assess the ability of actors across the sector to respond to a cyber incident in the UK, identifying gaps and areas for future improvement.[32] Participants include financial authorities, and representatives of the most systemically important firms.[33]

30 Food & Drug Administration, Precertification (Pre-Cert) Pilot Program: Milestones and Next Steps, as of 18 July 2019.

31 Food & Drug Administration, FDA Selects Participants for New Digital Health Software Pre-certification Pilot Program, as of 26 September 2017.

32 Bank of England, Sector Simulation Exercise: SIMEX 2018 Report, as of 27 September 2019.

33 Bank of England, Bank of England sector resilience exercise, as of 27 September 2019.

RECOMMENDATIONS FOR ENGAGEMENT & DISCLOSURE EXPECTATIONS

In a world where innovation and digital connectedness are critical to economic growth, it would be unwise to ignore threats to the shared digital environment. Cyber risk is a prominent one, given its systemic relevance and the potential severity of impact.

At an organisational level, cyber risk can undermine a company's ability to leverage data as a value driver, disrupt operations and reduce trust in products and services. Cyber events can also lead to network disruptions; due to the complex environments in which companies operate, the weaknesses in their infrastructure may not just result in threats to their own business but may also impact other actors in the digital ecosystem with whom they interact, such as suppliers, service providers and customers.[34]

In such a context, investor scrutiny around cyber risk management and governance is more important than ever. However, the technical nature of this risk may dissuade ESG and investment professionals from seeking an informed discussion with portfolio companies. To overcome some of the perceived barriers to effective engagement, the below provides tools and guidance for investors.

KEY RECOMMENDATIONS AND QUESTIONS FOR COMPANY ENGAGEMENT

This section sets out five high-level recommendations for investors and provides examples of questions that they can raise when engaging with companies on cyber security.

1. VALIDATE BOARD OVERSIGHT

As regulations on cyber security and data protection increase in reach and scope, there will be growing focus on how boards are fulfilling their fiduciary responsibilities around cyber resilience.[35] The extent of board buy-in on cyber security can also be a good litmus test for the effectiveness of a company's approach to cyber risk. Ownership at the management level and ad hoc reporting of incidents are no longer sufficient to respond to the ever-increasing and sophisticated challenges from high-impact cyber events. It is therefore critical for investors to validate oversight, competencies and accountability for cyber security at the board level.

Potential questions:

- What is the governance structure underpinning cyber security at your organisation, and can you demonstrate its effectiveness?
- Do you have board expertise on cyber security?
- How do you address gaps in skills and experience relating to cyber security on your board?

2. ENSURE CYBER RESILIENCE IS INTEGRATED INTO OVERALL STRATEGY

Cyber security plans cannot exist in a vacuum. In order to have a holistic position on cyber security, boards should integrate cyber risk into their enterprise risk management and consider implications for broader business decisions, e.g. relating to mergers and acquisitions, investments, value chain and the customer proposition. Investors should be asking companies about their thinking on strategic orientation when it comes to cyber resilience through preventative and compliance-oriented cyber defences.

Potential questions:

- What are your strategic and compliance priorities regarding cyber security?
- What are your key concerns about cyber security within your value chain?

3. CHECK FOR COMMON LANGUAGE

It is important that management information on cyber security is clear and accessible, rather than technical and jargon-heavy, and that there are measures and metrics in place to enable non-IT experts within the firm to evaluate and drive progress against expectations set by the board. Investors should review how board thinking on cyber is driven across the organisation by looking for inconsistencies between policies, benchmarks and incentives.

Potential questions:

- Could you provide examples of cyber security metrics reported to the board, and how these are linked to wider incentives and benchmarking across the company?
- How has board reporting on cyber security aided improvements in cyber security plans and strategy?

34 World Economic Forum (2020), The Global Risks Report 2020.

35 World Economic Forum (2017), Advancing Cyber Resilience: Principles and Tools for Boards.

4. LOOK BEYOND TECHNICAL CONTROLS

Cyber security concerns have led to an arms race for bigger and better technological solutions. However, cyber security is not just a technological challenge. Equal or even greater attention should be assigned to people, policies and processes. Indeed, a majority of data breaches within organisations are the result of human actors and preventative measures and infrastructure enhancements can only go so far if they are not properly integrated and utilised.[36] Investors speaking to portfolio companies should raise questions that provide insights regarding the priority accorded to cyber security and the extent of cyber security awareness.

Potential questions:

- What are your learnings from cyber security breaches you have experienced and how have you modified existing mechanisms to reflect these learnings?
- How are you strengthening organisational capacity as part of your cyber security defence?

5. SET DISCLOSURE EXPECTATIONS

One of the reasons that companies may not be effectively communicating their cyber security measures in the public domain is that may be unaware of investors' expectations regarding disclosure on the topic. Private dialogues with companies can enable candid conversations on the need for improved disclosure and address perceived barriers (e.g. concerns regarding greater exposure to attacks from increased disclosure). Investors can also set out what they deem as the minimum in terms of disclosure based on current reporting practices across sectors.

To support investor efforts, and based on our learnings from the collaborative engagement programme and research, we outline below a set of **disclosure expectations:** these can be used to identify gaps in company disclosure, benchmark portfolio companies against their peers, and as a tool for engagement to drive better disclosure on cyber security (see Box, Disclosure expectations).

DISCLOSURE EXPECTATIONS

The disclosure expectations refer to the indicators used in the engagement and have been broken down into three broad categories, based on the levels of public reporting among target companies as of 2019.

COMMON STANDARDS OF DISCLOSURE:

Includes three areas of company reporting that are well established. Within the research sample, over 80% of companies disclosed these indicators.

1. Commitment to legal compliance on cyber security and data protection (Indicator 1)
2. Data protection and privacy policy (Indicator 2)
3. Incorporation of cyber security into business continuity and risk management plans (Indicator 14)

EMERGING DISCLOSURE:

Identifies four areas where reporting is becoming more commonplace. Over 50% of companies in the research sample provided disclosure on these indicators.

4. Board committee responsibility for cyber security issues (Indicator 5)
5. Frequency and channels of communication of cyber security issues to the board (Indicator 6)
6. Internal or external cyber expertise, including through industry-wide collaboration (Indicator 9)
7. Financial capacity and team resources for cyber security (Indicator 8)
8. Incident management plan (Indicator 13)

AREAS FOR EXPANDED PUBLIC REPORTING:

Identifies two indicators that are basic and with no disclosure sensitivities but where, surprisingly, reporting among companies is below par.

9. Identification of named senior person or executive committee responsible for cyber security (Indicator 4)
10. Evidence of training on cyber security requirements to all staff (Indicator 11)

Other areas not currently incorporated in the minimum disclosure expectations but included in the initial benchmark research – such as audits (Indicator 12), extent of policy coverage (Indicator 3), board expertise on cyber (Indicator 10) and detailed board reporting (Indicator 7) – can be raised in private engagement conversations and be considered for future expectations.

36 ENISA (2017), Cyber Security Culture in Organisations.

NEXT STEPS

Cyber risk is an issue that will grow in complexity, especially given the unprecedent rate of wider technological advances and innovation. For example, the rapid advance of artificial intelligence technology is likely to add a new dimension to the threat, posing challenges for companies, investors and regulatory bodies alike.

Going forward, and building on this work, the PRI will explore related themes such as artificial intelligence and the ethics of innovation as well as appropriate governance mechanisms and regulatory gaps. To support investors in understanding related risks and opportunities and formulating their response, the PRI will also consider the broader implications of technology for sustainable development and responsible investment, looking across the entire investment chain.

CREDITS

AUTHORS:

Vaishnavi Ravishankar, PRI
Betina Vaz Boni, PRI
Athanasia Karananou, PRI

CONTRIBUTORS:

Nabylah Abo Dehman, PRI
Shelagh Whitley, PRI

EDITOR:

Mark Nicholls

DESIGN:

Will Stewart, PRI

The Principles for Responsible Investment (PRI)

The PRI works with its international network of signatories to put the six Principles for Responsible Investment into practice. Its goals are to understand the investment implications of environmental, social and governance (ESG) issues and to support signatories in integrating these issues into investment and ownership decisions. The PRI acts in the long-term interests of its signatories, of the financial markets and economies in which they operate and ultimately of the environment and society as a whole.

The six Principles for Responsible Investment are a voluntary and aspirational set of investment principles that offer a menu of possible actions for incorporating ESG issues into investment practice. The Principles were developed by investors, for investors. In implementing them, signatories contribute to developing a more sustainable global financial system.

More information: www.unpri.org

PRI Principles for Responsible Investment

The PRI is an investor initiative in partnership with UNEP Finance Initiative and the UN Global Compact.

United Nations Environment Programme Finance Initiative (UNEP FI)

UNEP FI is a unique partnership between the United Nations Environment Programme (UNEP) and the global financial sector. UNEP FI works closely with over 200 financial institutions that are signatories to the UNEP FI Statement on Sustainable Development, and a range of partner organisations, to develop and promote linkages between sustainability and financial performance. Through peer-to-peer networks, research and training, UNEP FI carries out its mission to identify, promote, and realise the adoption of best environmental and sustainability practice at all levels of financial institution operations.

More information: www.unepfi.org

UNEP FINANCE INITIATIVE

United Nations Global Compact

The United Nations Global Compact is a call to companies everywhere to align their operations and strategies with ten universally accepted principles in the areas of human rights, labour, environment and anti-corruption, and to take action in support of UN goals and issues embodied in the Sustainable Development Goals. The UN Global Compact is a leadership platform for the development, implementation and disclosure of responsible corporate practices. Launched in 2000, it is the largest corporate sustainability initiative in the world, with more than 8,800 companies and 4,000 non-business signatories based in over 160 countries, and more than 80 Local Networks.

More information: www.unglobalcompact.org

United Nations Global Compact