CONSULTATION RESPONSE

US SECURITIES AND EXCHANGE COMMISSION: CYBERSECURITY RISK MANAGEMENT, STRATEGY, GOVERNANCE, AND INCIDENT DISCLOSURE; RIN 3235-AM89

April 2022

This response represents the view of the PRI Association and not necessarily the views of its individual members.

PRI Association
Registered office: 5th floor, 25 Camperdown Street
London, UK, E1 8DZ Company no. 7207947
T: +44 (0) 20 3714 3220 W: www.unpri.org E:info@unpri.org

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

INTRODUCTION

The Principles for Responsible Investment (PRI) is the world's leading initiative on responsible investment. The PRI is a not-for-profit company with over 4,800 signatories (pension funds, insurers, investment managers and service providers) to the PRI's six principles with approximately US $121 trillion in assets under management.

The PRI supports its international network of signatories in implementing the Principles. As long-term investors acting in the best interests of their beneficiaries and clients, our signatories work to understand the contribution that environmental, social and governance (ESG) factors make to investment performance, the role that investment plays in broader financial markets and the impact that those investments have on the environment and society as a whole.

The PRI works 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.

ABOUT THIS CONSULTATION

The Securities and Exchange Commission (SEC or the Commission) is consulting on a series of proposed rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934.

The proposed amendments would require, among other things, current reporting about material cybersecurity incidents and periodic reporting to provide updates about previously reported cybersecurity incidents. The proposal also would require periodic reporting about a registrant's policies and procedures to identify and manage cybersecurity risks; the registrant's board of directors' oversight of cybersecurity risk; and management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures. The proposal further would require annual reporting or certain proxy disclosure about the board of directors' cybersecurity expertise, if any.

Cybersecurity is an important topic that investors seek standardized and transparent disclosure from public companies on. The PRI welcomes the opportunity to respond to the SEC's consultation.

For more information, contact:

Karen Kerschke
US Policy Analyst
[redacted]

Betina Vaz Boni
Senior Analyst, Governance
[redacted]

KEY RECOMMENDATIONS

The PRI welcomes the SEC's proposals requiring greater transparency around companies' cybersecurity practices. In the past, the PRI has encouraged signatories to consider cybersecurity risks because of the rising vulnerabilities of companies to cyber-attacks. A 2019 report from Accenture, for example, found that cybersecurity breaches had risen by over 65% over the last five years[1] and in 2020 the World Economic Forum identified cyber-related issues as one of the top ten long-term risks globally.[2] Internationally, cybersecurity has been recognized as a significant "threat to the integrity, efficiency and soundness of markets worldwide".[3] Harms caused by cybersecurity attacks can be financial (e.g. fall in stock price, regulatory fines and legal fees, revenue loss from operational delays), 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).[4]

The PRI's research on cybersecurity has focused on governance aspects of cybersecurity disclosure. Therefore, the PRI's response will focus on this topic, although we are broadly supportive of the proposed rule.

The PRI supports the inclusion of the following disclosure requirements:

- Disclosure of a registrant's policies and procedures for identifying and managing cybersecurity risks, covering especially the cybersecurity risks associated with its use of any third-party service provider.
- Disclosure of a registrant's cybersecurity governance, including board of directors' oversight of cybersecurity risks.
- Disclosure of a registrant's management's role and relevant expertise in assessing and managing cybersecurity risks and implementing related policies, procedures, and strategies.
- Disclosure of the cybersecurity expertise of members of the board of directors.

The PRI further recommends that the Commission require:

- Disclosure of the type and extent of training on cybersecurity to management and staff.

[1] Accenture (2019), *The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study* (2019), available at https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf.
[2] World Economic Forum, *The Global Risks Report 2020*, available at https://www.weforum.org/reports/the-global-risks-report-2020.
[3] IOSCO, *Cybersecurity in Securities Markets – An International Perspective* (April 2016), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf.
[4] University of Oxford, *Researchers Identify Negative Impacts of Cyber Attacks* (29 October 2019), available at https://www.ox.ac.uk/news/2018-10-29-researchers-identify-negative-impacts-cyber-attacks.

DETAILED RESPONSE

DISCLOSURE OF A REGISTRANT'S RISK MANAGEMENT, STRATEGY AND GOVERNANCE REGARDING CYBERSECURITY RISKS

The PRI welcomes the proposal requiring registrants to provide more consistent and informative disclosure regarding their cybersecurity risk management, strategy, and governance.

The proposed disclosures would meet investors' data needs on cybersecurity and governance. The PRI led research in the form of collaborative engagement from 2017 to 2019 on cybersecurity.[5] Representing over US$12trn in assets, 55 institutional investors engaged 53 portfolio companies from five different sectors to understand how they are demonstrating preparedness and addressing cyber-related risks, using governance as a proxy for resilience.

The engagement revealed that although companies are increasingly recognising cyber risks and their impacts, their public disclosures do not provide investors with the information necessary to evaluate whether companies have adequate governance structures and measures in place to deal with cybersecurity challenges.

The lack of public disclosure also hinders investor ability to differentiate between those companies that are proactively developing, monitoring and managing cybersecurity risks versus those failing to prioritise these risks. The Commission's disclosure proposals would allow investors to better assess company policies and control, accountability and board oversight related to cybersecurity.

Policies and procedures

We welcome the proposal requiring registrants to disclose their policies and procedures to identify and manage cybersecurity risks and threats. We are particularly supportive of the requirement to disclose the coverage of issuers' policies and procedures regarding third parties. **We encourage the SEC to clarify that disclosure of policies and procedures should include disclosure of the extent that policies cover global operations, not just those in the US.**

PRI's research demonstrated that while companies generally perceived cybersecurity as a key organisational risk, very few communicated that they have policies, governance structures and processes that were effective at tackling cyber threats.[6] The research also showed that even when the policies were published by the company, most companies did not include the extent of the coverage for global operations and third parties.

Comprehensive disclosure of cybersecurity policies is particularly valuable as associates in the value chain, including suppliers and vendors, are often viewed as weak links when it comes to cybersecurity; they hold or have access to sensitive data but may not have appropriate policies and processes in place.

---

5 Principles for Responsible Investment, *Engaging on cybersecurity: results of the PRI collaborative engagement 2017-2019* (2020), available at https://www.unpri.org/cyber-security/engaging-on-cyber-security-results-of-the-pri-collaborative-engagement-2017-2019/5680.article.

6 Principles for Responsible Investment (2018), *Stepping up governance on cybersecurity: what is corporate disclosure telling investors?* (2018), available at https://www.unpri.org/download?ac=5134.

The PRI engagement dialogues demonstrated a need for investors to establish systematic policies and processes addressing cybersecurity risks.[7] The proposed disclosure would support investors in managing cybersecurity risk as disclosure can show companies' readiness to address potential threats and the robustness of the steps being taken to manage cyber risks.

Governance and board oversight

The PRI welcomes the proposal requiring disclosure of a registrant's cybersecurity governance, including the board's oversight of cybersecurity risk.

Investors increasingly expect cybersecurity issues to fall within the remit of company boards and their sub-committees given the potential physical and economic implications of a cybersecurity incident on business operations.[8] The extent of board buy-in on cybersecurity can be a good litmus test for the effectiveness of a company's approach to cyber risk. Although companies may adopt different models, depending on what is most appropriate for their business and in line with existing governance structures, it is important that they communicate where ultimate responsibility for cyber issues sits within the company.

Boards have a role in ensuring that cybersecurity considerations are not just integrated into risk management, but that they also drive strategy and shape broader business decision making.[9] In order to enable this, board members should receive quality management information and be well-informed so that they can sense-check the adequacy of cybersecurity programs, and challenge management actions where appropriate.

The PRI's research revealed that companies often did not disclose details of which cybersecurity information is reported to the board and how this information is evaluated.[10] Investors engaging with issuers found that this level of information was critical to develop a view around the robustness of decision making on cybersecurity issues within the firm. As such, the Commission's proposed requirement disclosures would support investor efforts on this topic.

Management role

The PRI also welcomes the Commission's proposal requiring disclosure of management's role and relevant expertise in assessing and managing cybersecurity risks and implementing related policies, procedures and strategies.

As the number of cybersecurity incidents continues to rise, and take new forms, it is vital that companies have robust governance measures in place to manage and address risks. Having a person or committee directly accountable for cybersecurity risk is a key first step. Having a senior executive responsible for cybersecurity signals to investors that there is internal expertise to appropriately allocate investments, staff time and resources. Senior management is best placed to

---

[7] Principles for Responsible Investment, *Engaging on cybersecurity: results of the PRI collaborative engagement 2017-2019* (2020), available at https://www.unpri.org/cyber-security/engaging-on-cyber-security-results-of-the-pri-collaborative-engagement-2017-2019/5680.article.
[8] Ibid.
[9] Marsh, Governing Cyber Risk: A Guide for Company Boards (April 2018), available at https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/governing-cyber-risk-report.pdf.
[10] Principles for Responsible Investment (2018), *Stepping up governance on cybersecurity: what is corporate disclosure telling investors?* (2018), available at https://www.unpri.org/download?ac=5134.

manage cybersecurity on a day-to-day basis and keep the board aware of cybersecurity and related risk management.[11]

The PRI's research revealed that disclosure of management accountability for cybersecurity is lacking.[12] As investors are not privy to internal management discussions around cyber readiness or incident management, they rely on company boards and management for their oversight, governance and disclosure of this enterprise risk. The PRI supports the proposal, as the required disclosure would encourage companies to better articulate where responsibility for cybersecurity lies within the business.

DISCLOSURE REGARDING THE BOARD OF DIRECTORS' CYBERSECURITY EXPERTISE

The PRI welcomes mandatory disclosure of board expertise on cybersecurity. In general, the PRI believes that enhanced expertise at the board level on sustainability matters is crucial to companies' sustainability efforts. Board cybersecurity expertise serves as a useful starting point for investors to assess a company's approach to cybersecurity, which is one part of sustainable operations.

However, the existence of a cybersecurity expert on the board should not be used as a proxy for efficient cybersecurity risk management. Alternative approaches to addressing cyber expertise at the board level can be an important aspect of a company's risk management strategy. For instance, PRI research showed that companies have nuanced positions on board expertise on cybersecurity.[13] Many companies take alternative approaches to address deficits in knowledge and expertise on the board and ensure that board members are able to ask the right questions and challenge senior management on cybersecurity. Examples to upskill their boards on cybersecurity include training, support of external advisors and specialist consultants. Moreover, PRI's engagement dialogues revealed that companies 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. Therefore, we recommend that the disclosure requirement should be broadened to require disclosure on how board expertise on cybersecurity is addressed. With this change, issuers could report other ways cybersecurity expertise is addressed.

ADDITIONAL RECOMMENDATIONS

Training on cybersecurity

The PRI recommends the Commission require disclosure of the extent of management and staff training on cybersecurity.

---

[11] Council of Institutional Investors, *Prioritizing Cybersecurity: Five Investor Questions for Portfolio Company Boards* (2016), available at https://corpgov.law.harvard.edu/2016/05/20/prioritizing-cybersecurity-five-questions-for-portfolio-company-boards/.
[12] Principles for Responsible Investment, *Engaging on cybersecurity: results of the PRI collaborative engagement 2017-2019* (2020), available at https://www.unpri.org/cyber-security/engaging-on-cyber-security-results-of-the-pri-collaborative-engagement-2017-2019/5680.article.
[13] Principles for Responsible Investment, *Engaging on cybersecurity: results of the PRI collaborative engagement 2017-2019* (2020), available at https://www.unpri.org/cyber-security/engaging-on-cyber-security-results-of-the-pri-collaborative-engagement-2017-2019/5680.article.

Staff training is an important element of risk management, the 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 utilized across the organization.[14]

In fact, the PRI engagement revealed that although several companies implemented risk management training for all employees, they failed to disclose information on training on cybersecurity and data protection.[15] Cybersecurity processes and procedures should be embedded throughout the organisation and expanded through education and training for all staff. Details on training and education efforts should be properly disclosed, because providing regular training to all staff on cyber threats, handling sensitive information, IT policies and procedures is essential for effective governance of cybersecurity.

The PRI has experience of public policy on sustainable finance policies and responsible investment across multiple markets and stands ready to further support the work of the Commission on cybersecurity disclosure requirements.

Question or comments related to this response can also be sent to [redacted]

[14] European Union Agency for Cybersecurity, *Cybersecurity Culture in Organisations* (2017), available at https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.
[15] Principles for Responsible Investment, *Engaging on cybersecurity: results of the PRI collaborative engagement 2017-2019* (2020), available at https://www.unpri.org/cyber-security/engaging-on-cyber-security-results-of-the-pri-collaborative-engagement-2017-2019/5680.article.