PRESIDENT AND FELLOWS OF HARVARD COLLEGE
CORPORATION COMMITTEE ON SHAREHOLDER RESPONSIBILITY

OFFICE OF THE GOVERNING BOARDS
(617) 495-1534

LOEB HOUSE, 17 QUINCY STREET
CAMBRIDGE, MA 02138

Proxy Voting Guidelines for External Managers

Topic: **Technology and Media**
Subtopic: **Cybersecurity and data protection**
Approved: **June 8, 2022**

Description:

Resolutions on this topic ask companies to address cybersecurity and data protection by, for example, requesting a report explaining how a board oversees cybersecurity and data protection risks.

Topic background:

In certain sectors, cybersecurity and data protection are top enterprise risks for companies. The cost of failure can be significant. These risks will continue to present challenges for companies as malware and other tactics to breach company networks evolve.[1] The Value Reporting Foundation's SASB Standards highlight data security as material for companies in the consumer goods, financial services, food and beverage, technology and communications, healthcare, and aerospace and defense sectors. According to a report by IBM, the average cost of a data breach reached $4.24 million in 2021.[2] In addition to the direct costs, cybersecurity and data protection issues have resulted in reputational damage, affecting a company's relationship with employees and customers.

Companies should have a comprehensive understanding and appropriate board oversight of cybersecurity readiness including regular assessment of data loss prevention, vulnerability management, and anti-malware systems. Best practices may consist of maintaining and reporting KPIs such as number of attacks, cost per incident, or time to resolve. Data protection requires securing data or information against unauthorized access or use. Although we do not address data privacy, a separate but related issue, in this guideline it is important to note that data protection is a key factor in ensuring data privacy. Stakeholders look for evidence of strong data governance. Management should be able to explain where data resides and how access is controlled, including data provided by third parties. Beyond management, employee training is also an important component to managing cybersecurity risk and data protection. Investor

[1] The Cybersecurity & Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to United States cyber and physical infrastructure. Updates on cybersecurity matters are provided through its Shields Up initiative.
[2] The full IBM Report can be found here.

engagement on the topic of cybersecurity has resulted in improved company disclosure in proxy documents and other transparency reporting.[3]

Considerations for voting:

- In reviewing company-specific proposals, we consider (1) the risk of data breaches (2) how companies are responding to cybersecurity risk, data protection, and data privacy, and (3) how companies maintain oversight of this issue.
- In reviewing requests for companies to report or take action on cybersecurity risks, we seek to determine whether a company's current policies and practices are robust and whether the company may be lagging other industry participants or peers.
- Any shareholder requests for information on cybersecurity or data protection should be subject to existing laws and regulation and be provided at reasonable cost, not be overly burdensome, and omit proprietary information.

Illustrative examples of votes:

1. Vote in support of -a report explaining how the Board oversees cybersecurity and data protection risks.
2. Vote against requests for an overly prescriptive report or one that may result in undermining cybersecurity and data protection efforts by releasing sensitive data or highlighting specific areas of vulnerability.

Harvard offers broader general guidance on its recommended approach to considering shareholder resolutions in "Overview of Harvard University's Proxy Voting Guidelines for External Managers" (follow link to download full text). When determining votes on resolutions, we consider each resolution in light of this general guidance as well as in light of a resolution's specific request and contextual information about the relevant company and its approach to the issue.

[3] The Harvard endowment is a signatory to the UN PRI. More information on the PRI's work regarding cybersecurity and data protection, and investor engagement on the topic, can be found here.