RESEARCH REPORT

S&P 500 Proxy Statements: What Companies Disclose About Their Cybersecurity Programs

By Rob Sloan, VP Cybersecurity Advocacy, Zscaler

Investors are being short-changed when it comes to understanding how large-cap equities are managing and overseeing cyber risk. Despite increased discussion among regulators about what companies must disclose, an analysis of S&P 500 company proxy statements shows considerable variation in what investors are told.

The Securities and Exchange *Commission's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* rule, which passed in July 2023, has forced companies to consider how they communicate details of their cybersecurity program to potential and current investors. For many companies there is a lot of work to do.

Taking each S&P 500 company's most recent proxy statement as of February 16, 2024, 396 companies provided some level of information about the company's cybersecurity program — an average of 192 words. The breadth and depth of information shared varied widely with companies beginning to share more about the risks they face and the measures introduced to improve data protection, the detection and investigation of incidents, risk mitigation and transfer, employee training and awareness, and governance.

Of the remainder, seven companies disclosed no detail at all and a further 97 companies, 19% of the S&P 500, did not disclose any substantive detail about their programs beyond stating which committee oversaw the area.

Among those companies sharing additional information, a number of themes emerged:

- **Cybersecurity governance.** The vast majority of companies comment on how the board oversees cybersecurity and shares the name of the committee responsible. The data shows one in five broads is briefed by its chief information security officer on a quarterly basis, with only 2% of companies providing more frequent updates. Forty-two percent chose not to disclose a frequency and 25% opted for stating 'regularly' or 'frequently', but without further detail. Four percent were briefed 'at least annually,' though many investors might think this insufficient.

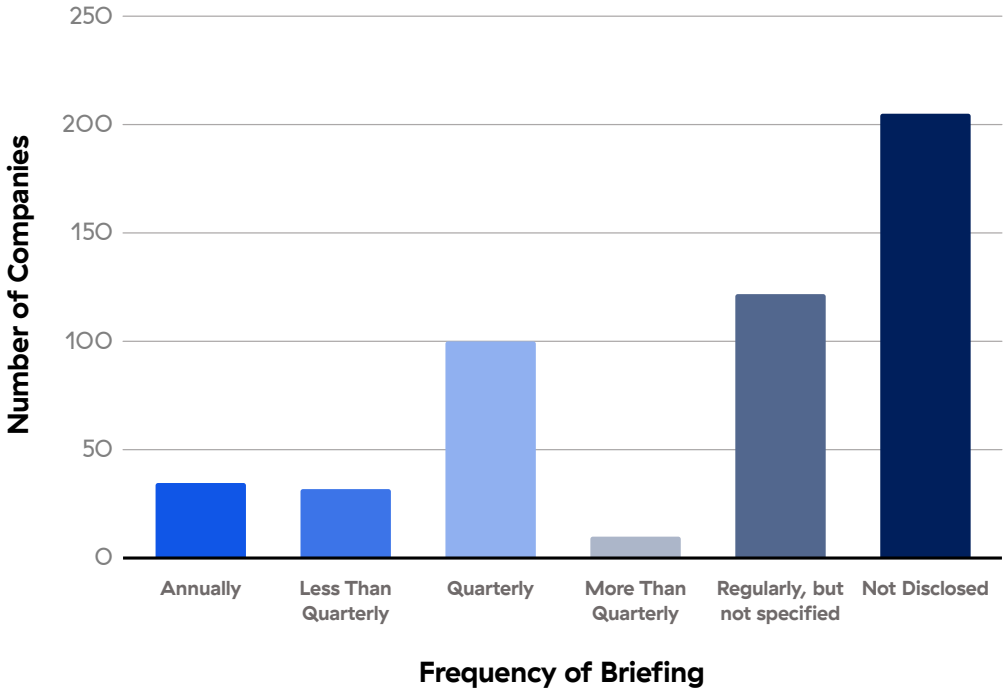

Figure 1: Frequency of CISO briefings to the board of directors, according to information in S&P 500 proxy statement filings.

- **Acknowledgement of cyber risk.** A minority of companies include an important statement to inform investors that the company is subject to cyberattacks that could have damaging consequences. For example, the APA Corporation highlights cybersecurity as a serious concern for the board because "more and more of our operations rely on digital technologies" and the "increasingly sophisticated" methods used in attacks "could pose serious risks to the Company's revenue, reputation, data integrity, and ability to operate in a safe and environmentally responsible way."
- **Adherence to industry best practices.** Following industry best practices around data security could give an investor confidence in a company's approach, but few reference this. Only 8% of S&P 500–listed companies state that they align with the National Institute of Standards and Technology (NIST) cybersecurity framework, and 4% mention attaining ISO 27001 or other ISO information security standards. Only four companies reference their journey towards zero trust: Caesars Entertainment, Albemarle, Dow, and VICI Properties, despite many more moving in that direction.
- **Material incidents.** An important indicator of a mature information security program is a lack of damaging incidents: Thirty–nine companies explicitly state that they have not had a material incident in a defined period, typically the previous three years. However, until late 2023, public companies were not obliged to disclose incidents, so we should not assume the remainder experienced no material incidents. Only four companies — Molson Coors Beverage Company, Westinghouse Air Brake Technologies, Vertex Pharmaceuticals, and Expeditors International of Washington — acknowledged having experienced an incident.

- **Director expertise.** Disclosing the levels of cyber expertise among individual directors did not make it into the final SEC rule, but listing relevant director qualifications signals a commitment to effective risk oversight. Some companies are sharing information via the board skills matrix, but only 17 companies included names of directors that had achieved relevant qualifications in proxy statements. The most commonly referenced qualification was the Cyber-Risk Oversight certificate from Carnegie Mellon University and the National Association of Corporate Directors.
- **Cyber insurance.** It is arguable how useful disclosing that a company has cyber insurance without knowing what is covered and to what value, but just under one in five companies, 18%, disclosed they maintain cyber insurance coverage. Some companies, including hotel chain Hilton Worldwide and media company Paramount Global, also state the type of insurance they carry. Real estate firm Public Storage is one of the few that provides context: "We believe we are adequately insured against losses related to a potential information security breach, and we maintain cybersecurity insurance coverage that we believe is appropriate for the size and complexity of our business."
- **Training and awareness.** One of the most popular disclosures, made by 32% of companies, was the existence of an employee cybersecurity training and awareness program. In particular, Equifax highlights how it provides employees with "customized training" and visibility into their own security performance. Further: "These performance measures are included in the calculation of annual incentive compensation for all bonus-eligible employees," the only company in the study that made such a disclosure.
- **Simulated attacks and responses.** Eight percent of companies mentioned incident response plans, but slightly fewer, 5%, said management and/or the board conducted tabletop exercises that simulated the response to attacks. Building product company Carrier Global described an "extensive tabletop exercise" carried out in 2022 with the CEO and senior executives. The exercise "simulated an enterprise wide ransomware attack [and] focused on identifying and closing potential gaps and areas of delay in our internal controls and response procedures."
- **Third-party risk.** Recently, several breaches have stemmed from supply chain attacks, but only 6% of S&P 500-listed companies included mentions of their third-party risk management efforts. Statements were typically short and lacked detail as to how the risk was managed. Advertiser Interpublic Group requires its third parties to "maintain security controls designed to ensure the confidentiality, integrity, and availability of our systems and the confidential and sensitive information we maintain and process." Pharmaceuticals company Zoetis has an "extensive third-party risk management program with a robust process for onboarding third parties."

Improving Future Disclosures

Corporate filings include more detailed information on cybersecurity programs now than ever, a reflection of the growing interest in cybersecurity among investors and regulators. And little wonder: cybersecurity incidents have the potential to severely damage a company's reputation and finances, disrupt operations, and result in significant regulatory penalties, any of which could affect the value of an investment.

Therefore, public companies should give serious consideration to disclosing more and giving investors a wider appreciation of the risks and how well prepared the business is to manage them. All companies should consider disclosing information that aligns with each of the nine categories above.

Ultimately, though, a standardized approach may be necessary to provide investors with the information they need in a digestible and accessible format that allows for easy comparison and uses a standard lexicon that is intelligible to all.

While regulatory change seems unlikely to drive such a change in the short term, investor demands for more information combined with a steady harmonization of filing content will raise the bar and benefit all.

To help board directors better understand cyber risk, Zscaler engaged CEO and Founder of Sand Hill East, Andy Brown, and professor at the Cox School of Business, Helmuth Ludwig, to create an essential resource: *Seven Steps for Boards of Directors, The Guide to Effective Cyber Risk Oversight*. Download it now here.

Meet the Author

Rob Sloan is the Vice President of Cybersecurity Advocacy at cloud security company Zscaler. Rob began his career in cybersecurity in 2002 working for the UK government and led some of the earliest investigations into state-sponsored cyber attacks before moving to a London-based security consultancy to set up and lead an incident response division. He joined Dow Jones and The Wall Street Journal in 2014 where he was tasked with helping an executive and board-director audience better understand cyber risk.

Write to Rob at:

rsloan@zscaler.com www.linkedin.com/in/robsloan1