RESEARCH REPORT

The SEC's Cybersecurity Rule Didn't Include Disclosure of Director Expertise. That Needs to Change

By Rob Sloan, VP Cybersecurity Advocacy, Zscaler

Director–level cyber expertise is an important consideration for potential investors of public companies, but an analysis of S&P 500 proxy statements shows fewer than one in five boards is adequately disclosing this information. Regulators and companies must take steps to improve disclosures of expertise and thereby reduce the risk of investors being misled about the capability of boards to oversee cybersecurity.

The research examined the skills matrices in the latest proxy statements of S&P 500 companies until mid–February 2024, almost two years after the Security and Exchange Commission's proposal of including a disclosure of board director cybersecurity expertise in its draft Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.

The proposed rule in March 2022 stated "the registrant would have to disclose the name(s) of any such director(s), and provide such detail as necessary to fully describe the nature of the expertise," because "investors may find disclosure of whether any board members have cybersecurity expertise to be important as they consider their investment in the registrant as well as their votes on the election of directors of the registrant."

When the rule was adopted in late July 2023, the expertise proposal had been dropped and investors lost out.

Key Findings

The analysis found 82% of S&P 500 companies included a skills matrix in their proxy statement, and more than half of all companies, 54%, included a category in the matrix that covered cybersecurity as a skill. However, far too often *cybersecurity* (or *information security*) was 'bundled' with another skill, such as *technology, information technology*, or *risk management*, which obfuscates the true expertise of the individual directors.

©2024 Zscaler, Inc. All rights reserved.

Bundling cybersecurity with other skills allows more directors to 'check the box' and may lead shareholders to mistakenly infer a board can effectively oversee cybersecurity risk.

Skills bundling allows directors to potentially only have one of several skills listed together. Companies typically use 'and' or a '/', between skills, which could lead investors to infer directors have both skills. Other companies use 'or' when bundling the several skills, for example a global information technology company that bundles *Technology, Cybersecurity or Digital*, which would allow virtually any director to check the box.

At best, this is unhelpful and requires further research from investors. At worst, it misleads shareholders into inferring a board is able to effectively oversee cybersecurity risk, when in reality it may not be able to do so.

Of the 500 companies, only 17% listed *cybersecurity* or *information security* as a skill in its own right. The information technology industry was most likely to list cybersecurity as a standalone skill. Forty-one percent of the 64 IT companies listed on the S&P 500 shared the number of directors with cyber expertise.

Among companies in the materials industry, including chemicals companies and metals & mining businesses, shareholders had less visibility of cyber expertise. Although each of the 28 companies shared a skills matrix in their respective proxy statement, 11 out of 12 companies bundled cybersecurity with other skills.

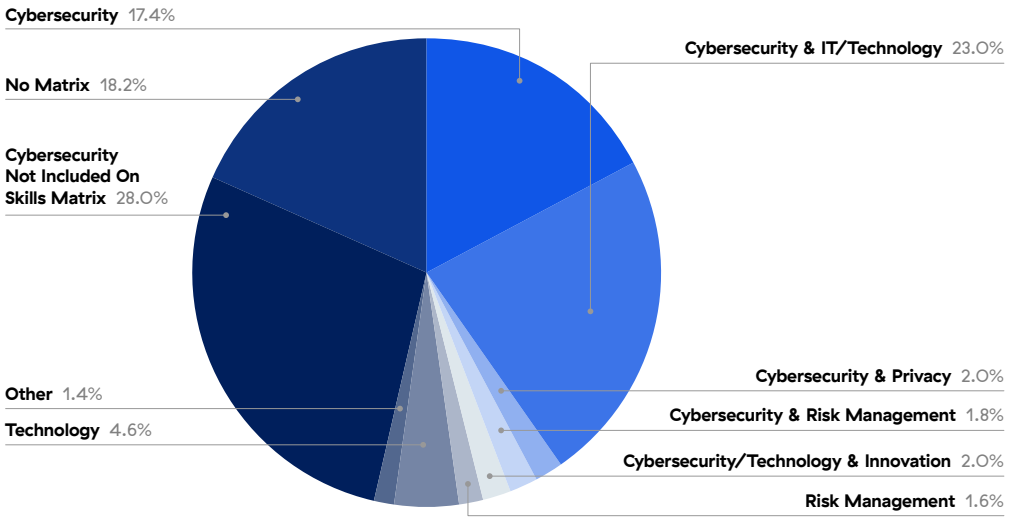

Figure 1: Only 17% of companies listed cybersecurity as a standalone skill on their matrix. Forty-six percent either chose not to share a skills matrix or did not include cybersecurity as a standalone or bundled skill.

Twenty-three percent paired *cybersecurity* with *information technology* and/or *technology*, while a small number of companies each paired *cybersecurity* with *privacy, risk management*, or *technology and innovation*. Last, 5% included cybersecurity as part of a collection of skills captured under the generic skill *technology* and a further 2% included it under a generic *risk management* skill.

©2024 Zscaler, Inc. All rights reserved.

Outliers

A handful of companies bundled cybersecurity skills differently from their peers:

- A beverages company disclosed directors with skills in *Technology, Data Analytics, e-commerce, Digital Marketing, and Cyber* ensuring a wide variety of skills directors could align with;
- An energy company included cybersecurity skill among *Congressional Engagement; National Security and Cyber Defense and Protection* — skills not typically bundled together;
- A real estate company included cybersecurity in the description of a very broad skill it termed *Experience in Other Boards or Management*. That skill was described as "prior board and/or governance experience, including risk management, cybersecurity or climate." Unsurprisingly, the matrix showed every member of the board had that skill.

How Bundling Affects the Average Number of Directors With Skills

When skills are bundled, more directors are able to check the box, which may give a false impression of the true level of cybersecurity expertise on the board.

Skills Matrix Category	Average Number of Directors
Cybersecurity	4.4
Cybersecurity & Privacy	4.4
Other	4.6
Cybersecurity & IT/Technology	5.1
Technology	5.8
Cybersecurity/Technology & Innovation	6.0
Cybersecurity & Risk Management	7.8
Risk Management	9.7

Figure 2: The average number of directors with skills in cybersecurity increases as the subject is bundled with other skills.

Proxy statements showed that across the 86 companies that listed cybersecurity on its own as a director skill, an average of 4.4 directors were proficient. In comparison to other research on director-level cyber expertise, this figure appears high.

Indeed, previous research I conducted for The Wall Street Journal in September 2023 found only 107 S&P 500 board directors had relevant cybersecurity experience in the previous 10 years. Seven of those directors had served as chief information security officers and many more had served as chief information officers to gain relevant professional experience.

©2024 Zscaler, Inc. All rights reserved.

Bundling cybersecurity with other skills (with the exception of privacy), resulted in an increase in the average number of directors fitting in the cybersecurity category: an average of 5.1 directors per board fulfilled the *cybersecurity & IT/technology* skill, while *cybersecurity & risk management* averaged 7.8 directors. Including cybersecurity as part of the generic *risk management* category allowed an average of 9.7 directors to claim proficiency.

Upskilling Directors

In addition to bundling, two additional methods were identified in the proxy statements that allowed companies to claim all or most directors had cybersecurity skills.

First, a number of companies defined several different levels of cybersecurity skill, ensuring that all directors had the skill to at least some degree. One aerospace and defense company stated all 10 directors were skilled in cybersecurity, though eight were graded only as 'competent', the lowest level of proficiency. One energy company stated four of its directors had attained skills through "exposure as a board committee member," which hardly counts as deep expertise.

Second, some companies claim directors have cybersecurity skills without providing any evidence. One industrials company states nine out of ten of its board directors have skills in cybersecurity, yet none of the directors' biographies in the proxy statement or in open source searches showed professional experience or qualifications.

Steps to Improvement

To avoid misleading investors, regulators and companies must take steps to improve clarity regarding cybersecurity expertise among board directors. It is not necessary for every director to be an expert in cybersecurity, but investors should rightly demand transparency on whether boards collectively have the skills to oversee cybersecurity risk effectively.

Have a clear definition of cybersecurity expertise and mandatory disclosure in annual SEC filings. Clearly defining cybersecurity as a board-level skill involves measuring directors' skills in four areas, any one of which could count: (a) whether directors have prior work experience in cybersecurity roles; (b) whether a director has had c-level responsibility for cybersecurity; (c) whether the director has a qualification in cybersecurity oversight from a recognized source; and (d) whether the director has other relevant knowledge or skills. Justifying why a director meets the grade would be substantially easier if regulators agree where the bar is set, as the SEC did for financial expertise in the Sarbanes-Oxley Act of 2002.

Cybersecurity should be a standalone skill on matrices. All public companies should be expected to include a skills matrix in proxy statements and cybersecurity should be a required skill alongside those that typically feature such as experience in corporate governance and financial expertise. Degrees of expertise and experience are not required, but rather directors should only be listed as skilled if they have significant experience, expertise, subject matter knowledge or a qualification.

©2024 Zscaler, Inc. All rights reserved.

Director biographies should provide additional details. Listing a director as a cybersecurity expert is not enough. The nature of the experience should then be expanded upon in the director's biography, including how recently the experience, expertise or qualification was gained.

Consideration for how other skills are represented. One skill barely represented on matrices is artificial intelligence, which has the potential to transform businesses. Directors need to ensure they are adequately equipped to understand the opportunities and risks AI brings and investors need assurance that the board is ready to drive progress and oversee managements' efforts.

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.

Methodology:

Data was accessed via the Securities and Exchange Commission's EDGAR database. The research considered the most current proxy statement for every company listed in the S&P 500 on February 16th, 2024. Every document was examined manually to account for the differences in how companies present skills information. Once the skill category which included cybersecurity was identified, either from the category name or its description, it was recorded along with the number of directors holding the skill. In the case of companies defining levels of a skill, all directors listed with any degree of proficiency were recorded. Once the skills were identified and extracted, they were grouped into similar categories to standardize skills definitions.

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

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.