RESEARCH REPORT

Board Committee Oversight of Cybersecurity

By Rob Sloan, VP Cybersecurity Advocacy, Zscaler

Recent Securities and Exchange Commission cybersecurity risk management rules have put a spotlight on how corporate boards oversee cybersecurity. An analysis of S&P 500 proxy statements and corporate governance documents shows 71% of large-cap U.S. equities oversee cybersecurity risk via the audit committee, but the picture varies significantly in some sectors.

The analysis found almost two-thirds (62%) of companies assigned cybersecurity oversight responsibility to the audit committee and a further 9% to committees that primarily focus on audit issues, most commonly the audit and finance or audit and risk committees.

The full board oversees cybersecurity at 41 companies, 8%, and 35 companies, 7%, oversee cybersecurity from a risk committee, or a committee where risk is the primary focus.

Minority of Companies Have Dedicated Cybersecurity Committee

Only 21 companies, just 4% of the index, oversee cybersecurity from a committee which lists its sole purpose, or one of its key responsibilities, as cybersecurity or information security. Seven of those companies operate in the information technology sector, five are categorized as consumer discretionary, and a further five are industrials.

One reason for this group having a cybersecurity-focused board-level committee may be that cybersecurity is something the company takes very seriously, but it is worth noting the formation of the committee may have been a response to a cybersecurity incident which had a significant impact on the company. In the last five years, over half of the 21 companies suffered a public data breach.

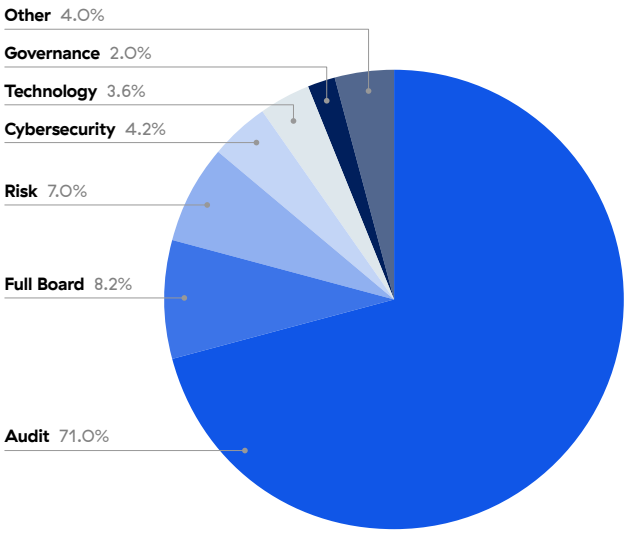

Figure 1: Oversight of cybersecurity at the board Level. Seventy-one percent of companies oversee cybersecurity risk from the audit committee.

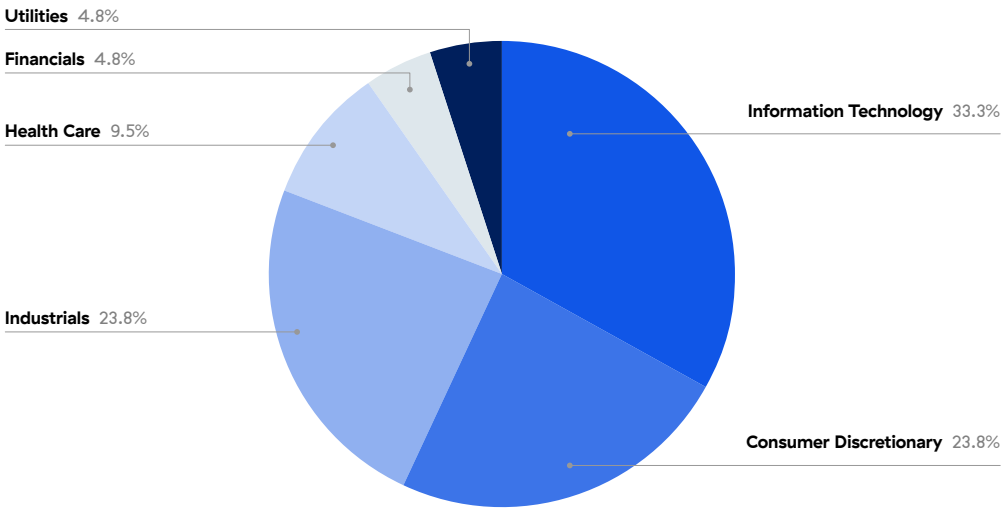

Figure 2: Industry breakdown of companies with a cybersecurity committee. One-third of companies with a committee focused on cybersecurity risk are in the information technology sector.

Industry Sector Differences

Although cyber risk oversight in most industries and sectors reflects the broader picture across all 500 companies, there are some differences. For instance, of the 23 S&P 500 companies operating in the energy industry, including 20 oil and gas companies, all but one oversee cybersecurity from the audit committee, the highest proportion of any industry in the study. The exception, APA Corporation, considers cyber risk an issue for the full board.

In contrast, the 72 S&P 500–listed companies that comprise the financial services industry approach cybersecurity risk oversight quite differently. Financials are most likely to oversee cyber risk from the risk committee (or a committee which has risk management as a key responsibility). Less than 40% of financials oversee cybersecurity from the audit committee and 11% give the issue full board oversight. Only one financial services business, payments and spend management company, Fleetcor Technologies, has a cybersecurity-focused committee, the *Information Technology and Security* committee.

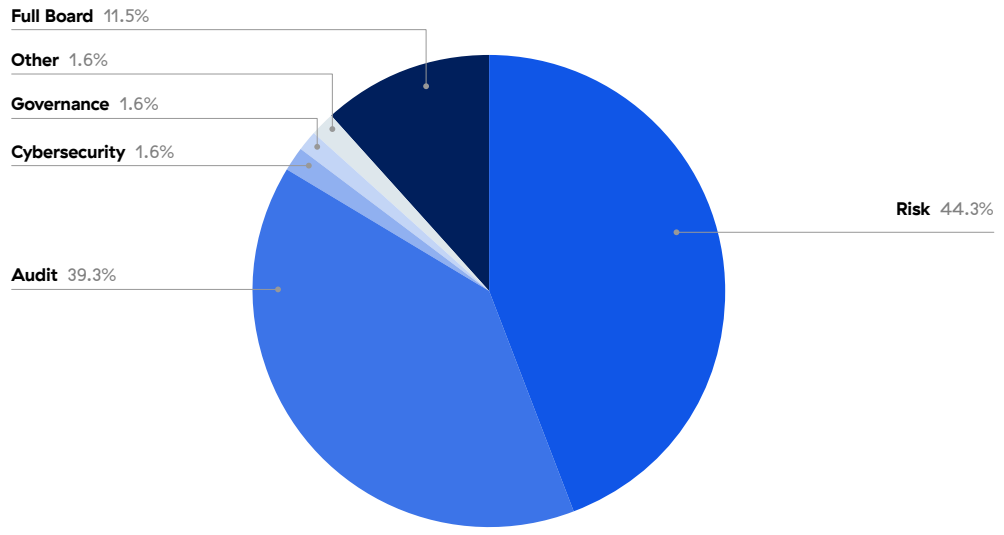

Figure 3: How financial services companies oversee cyber risk. Oversight from the risk committee is most common.

For banks, the audit committee has no role to play in cybersecurity oversight. Not a single one of the 15 banks listed in the index oversees cybersecurity from the audit committee. More than half, 53% oversee it from the risk committee, 40% oversee it from the technology committee, and most of the remainder oversees cybersecurity risk at the full board level.

Finally, among the 11 aerospace and defense companies on the index, no single approach dominates. Four oversee it from audit–focused committees and three from a cybersecurity–focused committee. Of the three largest U.S. defense contractors, Lockheed Martin and General Dynamics oversee cyber risk at the full board level, while the third, RTX Corp (Raytheon) oversees it from a *'Special Activities'* committee.

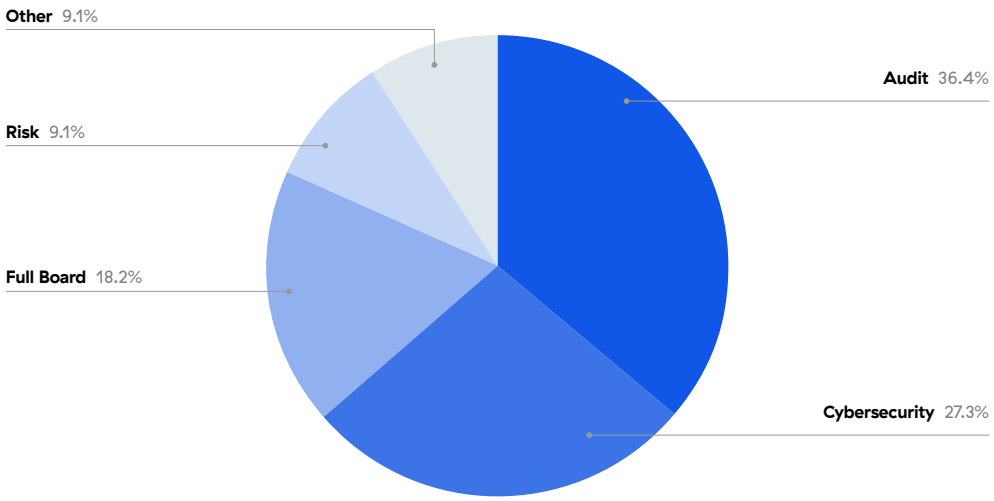

Figure 4: A mixed picture for cybersecurity oversight at aerospace and defense companies. Three of the 11 companies have a committee focused on cybersecurity.

No One–Size–Fits–All Approach

Boards can no longer ignore the issue of cybersecurity, nor did this research of larger companies find any evidence to suggest that was the case. The SEC's rule, adopted on July 26, 2023, provides clarity on what is expected of boards with respect to cybersecurity risk management, strategy, governance, and incident disclosure.

Indeed, given the recent changes and the scrutiny corporate cybersecurity is receiving from regulators, shareholders, the media and the public, there is a strong argument that cybersecurity is an issue that the full board should oversee. Among the 41 S&P 500 companies that agree are Microsoft, JP Morgan Chase, Alphabet, McKesson, and Pepsi.

Full board oversight allows all of the directors to participate in discussions and hone their cybersecurity oversight expertise. The National Association of Corporate Directors Cyber Risk Oversight Handbook (here) also highlights the breadth of cyber: boards should consider the topic as part of many issues presented to the board, including "discussions of new business plans and product offerings, mergers and acquisitions, new market entry, deployment of new technologies, major capital investment decisions such as facility expansions or IT system upgrades, and the like."

Ultimately though, the committee that oversees cybersecurity is secondary in importance to the actions being taken by directors to ensure management is acting responsibly and the cybersecurity program is effective in reducing risk and mitigating damaging incidents. Directors must ensure that they feel adequately briefed on the organization's exposure to cyber risks, understand how incidents will be dealt with, and have assurance the board and management are prepared from having simulated incidents.

As directors feel confident that cybersecurity risk is being well managed, the subject will likely move to a routine item on the audit or risk committee's agenda. Boards also face the same question about the best way to see other current and emerging issues such as environmental, social and governance topics and artificial intelligence. A standalone committee may be the best approach for the short term, but they too will become business-as-usual topics at some point.

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:

The research used the current (as of February 16, 2024) proxy statements for each of the S&P 500 companies as well as committee charter documents available on corporate websites to determine which committee had oversight of cybersecurity risk. In cases where several committees oversaw different aspects of cybersecurity, the primary committee was used. If you have questions, please email me at rsloan@zscaler.com.

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**.