WSJ PRO CYBERSECURITY RESEARCH

Survey Results Part Two: Directors Must Drive Cybersecurity Improvements

By Rob Sloan , Research Director , and WSJ Pro Research

March 17, 2023 5:19 pm ET

Key Points:

- Board directors largely have confidence in management to effectively deal with cyber risk. Sixteen percent rated management 'excellent' and 43% rated management 'very good'.
- Directors are only setting the agenda for their cyber briefings in a small minority of cases, possibly suggesting they do not know the information they need to conduct effective risk oversight.
- Boards that are briefed by the CIO or CISO are more likely to report an ability to use that information to effectively oversee cyber risk.
- Tabletop exercises involving cyber scenarios are lacking. Less than half of all respondents said their board had participated in one or more during the last 12 months.

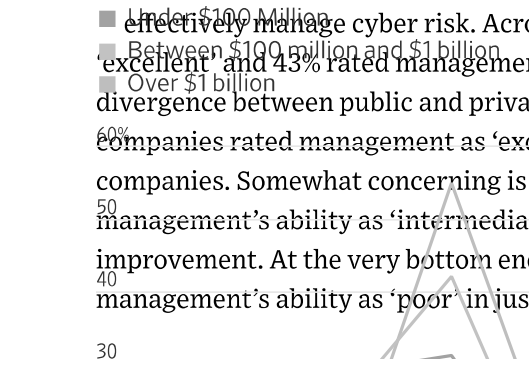
Background:

WSJ Pro, The Wall Street Journal's professional arm, collaborated with The National Association of Corporate Directors to gather survey responses from 472 corporate board directors on the current state of cybersecurity risk management expertise and preparedness to deal with cyber attacks.

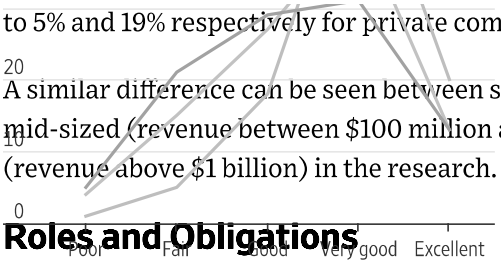
This research also provides a snapshot ahead of coming rule changes by the U.S. Securities and Exchange Commission that will require public companies to make standardized disclosures on cybersecurity risk management, strategy, governance, and incident reporting, as well as reporting cybersecurity expertise among board directors.

Rating Management's Abilities

Directors participating in the survey were asked to rate management's ability to effectively manage cyber risk. Across all respondents, 16% rated management as 'excellent' and 43% rated management as 'very good', but we saw considerable divergence between public and private companies. Fifty-one percent of private companies rated management as 'excellent' or 'very good' compared to 71% of public companies. Somewhat concerning is the fact that 41% of directors assessed their management's ability as 'intermediate', 'fair' or 'poor', leaving considerable room for improvement. At the very bottom end of the scale, public board directors rated management's ability as 'poor' in just 0.4% of cases and 'fair' in 7% of cases, compared



to 5% and 19% respectively for private companies.



A similar difference can be seen between smaller (annual revenue under $100 million), mid-sized (revenue between $100 million and $1 billion) and larger companies (revenue above $1 billion) in the research.

Roles and Obligations

Where confidence in management's ability to manage cyber risk may be lacking, an understanding of the board's role and obligations related to addressing a cyber crisis largely appears to be less of an issue in most cases. Overall, 84% of directors (91% of public companies and 79% of private company directors) were 'very or somewhat clear' on their duties. Technology and larger companies scored best at 95% and 93% respectively, dropping to 84% for mid-sized companies and 73% for smaller businesses.

The worst performers among the industries we analyzed were energy and utilities companies, 21% of which said they were 'not very clear' or 'not at all clear' on the board's role and obligations in addressing a cyber crisis, and professional services companies (26%).

Delivering The Briefing

Boards can only oversee cyber risk properly if they receive effective briefings from management. The survey asked which executive is responsible for briefing the board on cyber risk.

The executive delivering the risk briefing can have a profound effect on the information the board is given and the answers the directors get to their questions. The data showed public company boards are more likely to be briefed by either the chief information security officer (44%) or chief information officer (33%) than private company boards (28% and 26% respectively). The chief financial officer and chief executive officer are also responsible for briefing boards; 8% and 7% respectively in public companies, 8% and 22% in private companies.

Who Delivers the Cyber Risk Briefing?

Executives responsible for briefing the board on cyber risk.

EXECUTIVE DELIVERING BRIEFING	PRIVATELY OWNED	PUBLICLY LISTED
Chief Executive Officer	22%	7%
Chief Information Officer	26%	33%
Chief Information Security Officer	28%	44%
Chief Financial Officer	8%	8%
Chief Legal Officer	2%	2%
Chief Risk Officer	5%	3%

NACD & WSJ Pro Research

For the largest public companies in the survey, the CISO delivered the briefing almost half the time (48%), followed by the CIO (35%). The CEO led only 3% of the time.

There is a strong correlation between the executive who delivers management's cyber risk briefing and the board's ability to use that information to effectively oversee cyber risk. Ninety percent of larger businesses that have a CISO or CIO deliver the cyber risk briefing agreed that the information allows them to effectively oversee cyber risk. The figure fell to 74% of mid-sized companies and just 67% of smaller businesses.

The quality of board briefings may be a product of the agenda, and results varied very little among the various industries and business sizes we looked at. On average, just under two-thirds of respondents (64%) said both the board and management set the agenda and in almost a third of cases (32%), management sets the agenda. Only in a small minority of cases (4%) does the board set the agenda for the information it wants to hear, which might be an indicator that many boards are not certain of the information they need to conduct effective oversight of risk in this area.

Only 15% of respondents said that establishing a productive relationship with the management team on cyber is a significant challenge for their board, though this was somewhat higher for small businesses (24%) and consumer goods and retail companies (19%). Almost a third of respondents (32%) said the reporting of appropriate metrics from management is a challenge. This was especially the case for privately-held financial services companies (44%).

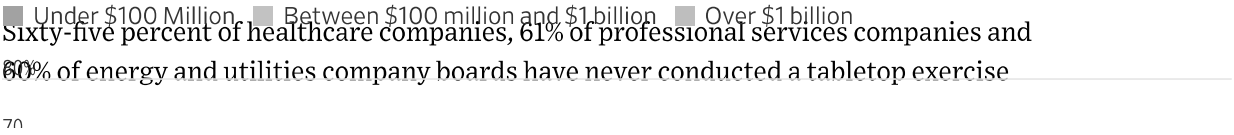
Regulatory Requirements for a Material Incident

The survey asked participants how clear the board is on SEC reporting and disclosure requirements following a material cyber risk or incident. Among the largest public companies in our survey, 50% said they were 'very clear' and a further 45% said they were 'somewhat clear'. These combined totals fell to 81% for mid-sized public companies and 60% for smaller companies. Respondents from the industrial and manufacturing sector and financial services sector were leaders, with 96% and 94% respectively 'very' or 'somewhat clear.' On the other hand, 15% of professional services and HR company directors and 13% of energy and utilities company directors were 'not very clear' or 'not at all clear'.

"Tabletop exercises" are recommended by cyber experts as a way for board directors to gain a better understanding of the regulations with which their companies need to comply and the decisions they will need to make during a cyber incident. A simulated scenario-based discussion where participants discuss and test their responses to hypothetical scenarios can help organizations and individuals evaluate crisis management plans, identify gaps, and improve response capabilities.

However, less than half of all respondents (48% for both public and private companies) said their board had taken part in a tabletop exercise related to cyber attacks.

Only 9% of private businesses and 7% of public companies carried out exercises twice a year or more and a further 25% of private company boards and 29% of public boards had carried out an exercise in the last 12 months. Thirteen percent and 11% respectively have conducted tabletop exercises, but not in the last 12 months.

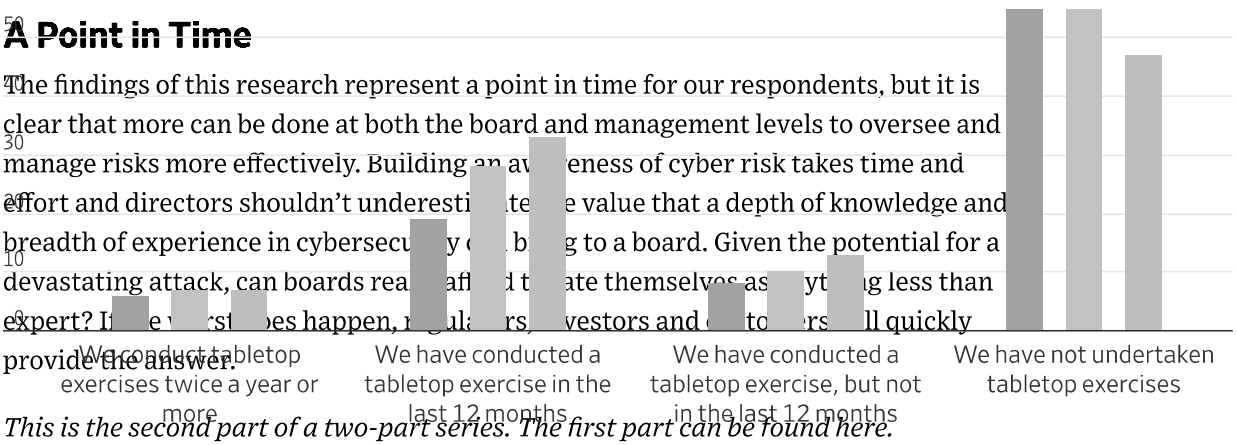


Sixty-five percent of healthcare companies, 61% of professional services companies and 60% of energy and utilities company boards have never conducted a tabletop exercise

around cybersecurity incidents, which could leave them wholly unprepared for how to respond to an attack.

A Point in Time

The findings of this research represent a point in time for our respondents, but it is clear that more can be done at both the board and management levels to oversee and manage risks more effectively. Building an awareness of cyber risk takes time and effort and directors shouldn't underestimate the value that a depth of knowledge and breadth of experience in cybersecurity can bring to a board. Given the potential for a devastating attack, can boards really afford to relate themselves as anything less than expert? If the worst does happen, regulators, investors and customers will quickly provide the answer.



This is the second part of a two-part series. The first part can be found here.

WSJ Pro Research is a premium membership that supports executive decision making on critical business issues by supplementing the news with timely, in-depth research and data.

All WSJ Pro Cybersecurity research reports, webinars, events and data are available at wsj.com/pro/cybersecurity/research

Meet the Author

Rob Sloan is research director at WSJ Pro. Rob joined Dow Jones in 2014 and spent several years with the Risk and Compliance product team before moving to The Wall Street Journal newsroom to develop and lead the WSJ Pro Research team.

In Rob's current role he manages a team of researchers, writes about cybersecurity, works on data projects and regularly presents on WSJ Pro events. Previously, Rob worked as response director for a specialist IT security consultancy in London, where he built a team focused on detecting, investigating and protecting against cyber intrusions and responding to incidents. Rob started his career working for the U.K. government, looking at some of the earliest state-sponsored cyberattacks against the critical national infrastructure.

Rob's main interest areas include the role of the board in overseeing and managing cyber risk, cybersecurity communications, the requirements of state-level attackers and helping corporate hacking victims share their lessons learned.

Write to Rob at rob.sloan@wsj.com

RELATED PAPERS

- Organizations Must Prepare for Revised Extortion Tactics (March 29, 2023)
- ChatGPT and Possible Cyber Benefits (March 24, 2023)
- Survey Finds Boards Have Work To Do on Cybersecurity: Executive Summary (March 20, 2023)
- Survey Results Part One: Board Directors Have Work To Do on Cybersecurity (March 17, 2023)
- ChatGPT and Cyber Risk (March 8, 2023)