Harness Your Company's Diversity for Strong Cybersecurity

Team @ Nasdaq Governance Solutions

Cybersecurity is a complex and difficult field. New threats are constantly emerging and malicious parties are growing more sophisticated. These attacks may lead to increased costs and legal issues as well as impact brand perception, customer loyalty, and overall shareholder value.

As more high-profile cybersecurity incidents occur, and as associated costs grow, boards are increasingly aware that cybersecurity risks are an existential threat to long-term business sustainability. However, it may be a struggle to find experienced leadership and directors to ensure cybersecurity is prioritized throughout their organizations.

A Nasdaq 2019 research report, Boards Through the Lens of Cybersecurity, uncovered interesting correlations between director age and gender, and cybersecurity, risk, and technology expertise. Per the findings, organizations with diversified boards may have a stronger foundation for more successful, long-term cybersecurity strategies.

How Cybersecurity is Changing the Boardroom

Disruptive, digital-first organizations are transforming industries and setting new customer expectations. Organizations are adding new directors to their boards with specific areas of technical expertise and experience. One or two specialists may not be sufficient as digital initiatives become important for organizations and functional areas. Additionally, this increased focus on digital initiatives goes hand-in-hand with investment in cybersecurity.

Although few S&P 100 companies analyzed had a separate board committee focused on cybersecurity, **most (88%) had charged at least one board-level committee with cybersecurity oversight**, according to the Nasdaq's 2019 research report- "Boards Through the Lens of Cyber-security". These findings suggest that organizations are zeroing in on cyber risk as a critical business issue.

88%
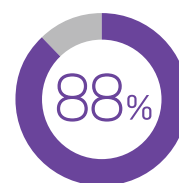
Companies in sectors like financial services and healthcare, which have access to sizable amounts of sensitive data, may find it helpful to have at least one "cybersecurity expert director" (as suggested in Nasdaq's 2019 research report mentioned above) in the boardroom to strengthen how the board understands, discusses, and addresses cyber risks. Companies face growing demands from policymakers, customers, and even their own employees to strengthen operational resilience and improve customer data security. A serious data breach or

cybersecurity lapse may lead to more than just bad publicity: It may have a negative impact on stocks, lead to sizable fines, or cost millions in lost revenue.

Cybersecurity experts are becoming vital members in the boardroom. They help guide board conversations by supporting directors in their due diligence and staying in tune with related issues and developments. Most of all, they help raise issues and present ideas that may guide the longer-term direction of the business.

Diversity's Potential Impact on Cybersecurity Oversight

As technology-based disruption grows, business leaders are prioritizing diversity to ensure they have the expertise required to identify and mitigate cyber risk.

In reviewing directors serving on boards who are charged with cybersecurity oversight, the Nasdaq Center for Corporate Governance found that a majority of directors fall in the 50 to 63 age group. **Directors under the age of 50 made up less than 5%**, and most of these were recent appointments with two or fewer years of board tenure.

5%
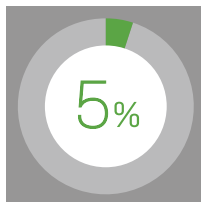
The report indicates that there is also a lack of women in cybersecurity director roles. Women currently account for only one-third of S&P 100 cybersecurity oversight directors, even though they appear to bring more cybersecurity and technology experience to the table. Nearly half of the women directors were described as having cybersecurity or technology expertise, compared to one-third of their male counterparts.

Cybersecurity needs are constantly changing, which has raised awareness of the need for boards to have qualified people to ensure strategies are sound. Boards may miss an opportunity to take their company's cybersecurity strategies to the next level if they do not encourage age and gender diversity amongst their board members.

The article has been authored for **Nasdaq Governance Solutions** by their internal team.

Nasdaq Governance Solutions supports organizations worldwide with innovative corporate governance and compliance solutions. Ranging from board portal technology to board engagement services to expert insights; these solutions are designed to help boards, leadership teams, corporate secretaries, and general counsel optimize their collaboration activities and drive governance excellence. Nasdaq's board portal software - Nasdaq Boardvantage®, helps enhance the effectiveness of virtual meetings, collaboration, and decision-making processes to drive business forward for your organization.

Takeaways for the Board

A strong company culture that prioritizes cybersecurity begins largely with the board. Giving the right people a seat at the table begins with the decisions of a company's directors and executive leadership. This includes embracing diversity and looking for experienced directors across genders, age groups, and areas of expertise.

Boards need a collaborative space to evaluate where diversity could benefit such elements as board and committee composition and structure, oversight processes, and reporting processes.

Nasdaq's corporate governance solutions—including Nasdaq Boardvantage®—are designed to help improve the board's ability to evaluate composition, begin to enrich discussions around cybersecurity strategies, and work together more efficiently, productively, and strategically.

> Cybersecurity experts help guide board conversations by supporting directors in their due diligence and staying in tune with related issues and developments.