Cybersecurity and the Board

Cybersecurity is getting increased scrutiny from boards across industries, as the threat of breaches and other online security-related issues pose significant risks. According to IT Governance, 95 security incidents around the globe compromised almost 66 million records in the first month of 2022 alone — impacting organizations across the industry spectrum, from banks and retailers to schools and hospitals.

Meanwhile, geopolitical tensions have raised the specter of government-sponsored cyber incursions on private-sector companies, which may find themselves in the middle and at risk. Regulatory bodies are taking notice, recognizing the materiality of cyber risk (and the risk to investors) wanting to ensure that boards and leadership teams are giving it proper oversight. For example, a recent proposal by the Securities and Exchange Commission (SEC) would require companies to disclose their oversight of cybersecurity as well as the cybersecurity expertise of their board members, which the SEC defines as prior work in cybersecurity; certification or a degree in cybersecurity; and/or knowledge, skills or other background related to cybersecurity.

More boards similarly recognize cybersecurity as a priority, beyond identifying and managing breaches. They see it as an integral component of their organizations' financial security, operational resiliency and brand reputation. These trends have boards interacting more frequently with chief information officers (CIOs) and chief information security officers (CISOs) in pursuit of a holistic view of the company's technology environment, the potential risks that exist, and the remediation plans, controls and processes in place for responding to a major breach.

Boards are also reflecting on how they can play a more effective governance role in helping their organizations manage cybersecurity risk. Some are seeking new directors with cybersecurity expertise to strengthen their position. But what exactly is the "right" expertise? And what backgrounds are best for a company's individual situation? In this article, we examine these questions and the key composition considerations as boards aim to build up their overall knowledge of cybersecurity.

The attributes of the cybersecurity-expert board director

Data from the most recent *U.S. Spencer Stuart Board Index* points to the overall lack of true technology expertise — let alone specific cybersecurity expertise — added to boards on the S&P 500. Of the 456 new independent directors who joined S&P 500 boards in 2021, only 18 (3.9 percent) have experience leading a function such as cybersecurity, IT, software engineering or data and analytics. The bulk of these new directors were brought on boards either at tech-centric companies, or by those facing regulatory scrutiny and higher-than-normal risk from breaches due to the sensitive nature of the information they manage, such as banks, insurers and healthcare companies.

For boards considering adding directors with technology and cybersecurity expertise, it is important to understand what backgrounds and qualifications are most effective when recruiting directors.

- **Technical expertise**. A deep understanding of and background in technology — including digital, technology transformation or emerging innovations — are certainly critical for this prospective board member. Directors should have the technical depth to be able to ask second-order questions of the CISO about the organization's true readiness, its need for investment and where to focus its resources. This is typically found in executives who have served as chief information, information security or technology officers, and/or have STEM degrees.
- **An ability to see the big picture**. Given how recently cyber risk has arisen as a board priority, many technology and cybersecurity experts lack previous board experience. Thus, it is critical that these potential first-time directors can elevate from the granular, technical details to the broader enterprise level. They will ideally have served on a company's executive leadership team and almost certainly will need experience presenting and reporting to boards.
- **More to offer**. Cybersecurity's importance is reflected in the increased visibility of CIOs and CISOs before the board. But on the board itself, there is obviously more at play than cybersecurity issues. A more additive board member would be a technical executive who has grappled not only with cybersecurity, but also with the role of technology in bigger strategic issues (e.g., driving revenue growth or increasing operational efficiency.)

Our work helping boards increase their cybersecurity capabilities has shown that the right candidate can be found by balancing the tradeoffs best for your individual situation (see figure). A CISO is most likely to have the necessary technical depth yet may have a more limited board background; a CEO of a technology or cybersecurity product company may have both board and technology leadership experience, but less exposure to the technical nuts and bolts. Public-sector leaders may have the connections to government agencies and law enforcement, but also less expertise on commercial topics and non-security issues.

CANDIDATE POOL TRADE-OFFS

	Pros	Cons
Chief Information Security Officer	» Deepest cybersecurity expertise; up-to-date knowledge on latest trends and issues » Connected with relevant government agencies, law enforcement and CISOs across different companies » Likely have experience presenting/reporting to risk/audit committees of boards	» Unlikely to have public board experience » May lack breadth of perspective beyond cybersecurity topics » Unlikely to have reported to a CEO and/or served on executive committee
Chief Technology/ Information Officer	» Deep cybersecurity expertise; likely directly managed CISOs and up-to-date on latest topics » Can contribute to board discussion beyond cyber (e.g., digital transformation, innovation) » Likely have experience presenting/reporting to audit committees of boards	» Less likely to have served on a public board than other executive committee positions
Security Industry Chief Executive Officer/ General Manager	» General knowledge of security topics as a product/services leader » Most "board-ready"; most likely to have previous experience serving on or presenting to the board » Able to contribute to board discussions beyond cyber (e.g., revenue growth, finance, etc.)	» May lack the technical depth and true subject matter expertise in cybersecurity topics
Public Sector/Military	» General knowledge of security topics in the context of the public sector (e.g., military, law enforcement, etc.) » Well-connected with relevant government agencies and law enforcement	» Likely lack public board experience » Likely lack private-sector experience more broadly » Less likely to contribute beyond security discussion at the board level

The right kind of tech experience

Cybersecurity has become a central priority for companies across industries, and with bottom lines and reputations at stake, boards cannot afford to play a passive role. Boards are catching up with respect to increasing cybersecurity expertise and their ability to effectively govern under the anticipation of cyber threats.

And as they seek new board members with the right technical and cybersecurity expertise, taking a smart and measured approach to adding directors can ensure they are ready to better support their organizations' security and resiliency going forward.

SpencerStuart

Authors

Julie Daum (New York), **Kate Hannon** (New York) and **Eric Zakre** (New York)

About Spencer Stuart

At Spencer Stuart, we know that leadership has never mattered more. We are trusted by organizations around the world to help them make the senior-level leadership decisions that have a lasting impact on their enterprises, on their stakeholders and the world around them. Through our executive search, board and leadership advisory services, we help build and enhance high-performing teams for select clients ranging from major multinationals to emerging companies to non-profit institutions.

Privately held since 1956, we focus on delivering knowledge, insight and results through the collaborative efforts of a team of experts — now spanning more than 70 offices, over 30 countries and more than 50 practice specialties. Boards and leaders consistently turn to Spencer Stuart to help address their evolving leadership needs in areas such as senior-level executive search, board recruitment, board effectiveness, succession planning, in-depth senior management assessment, employee engagement and many other facets of culture and organizational effectiveness, particularly in the context of the changing stakeholder expectations of business today. For more information on Spencer Stuart, please visit **www.spencerstuart.com**.

Social Media @ Spencer Stuart

Stay up to date on the trends and topics that are relevant to your business and career.

@Spencer Stuart