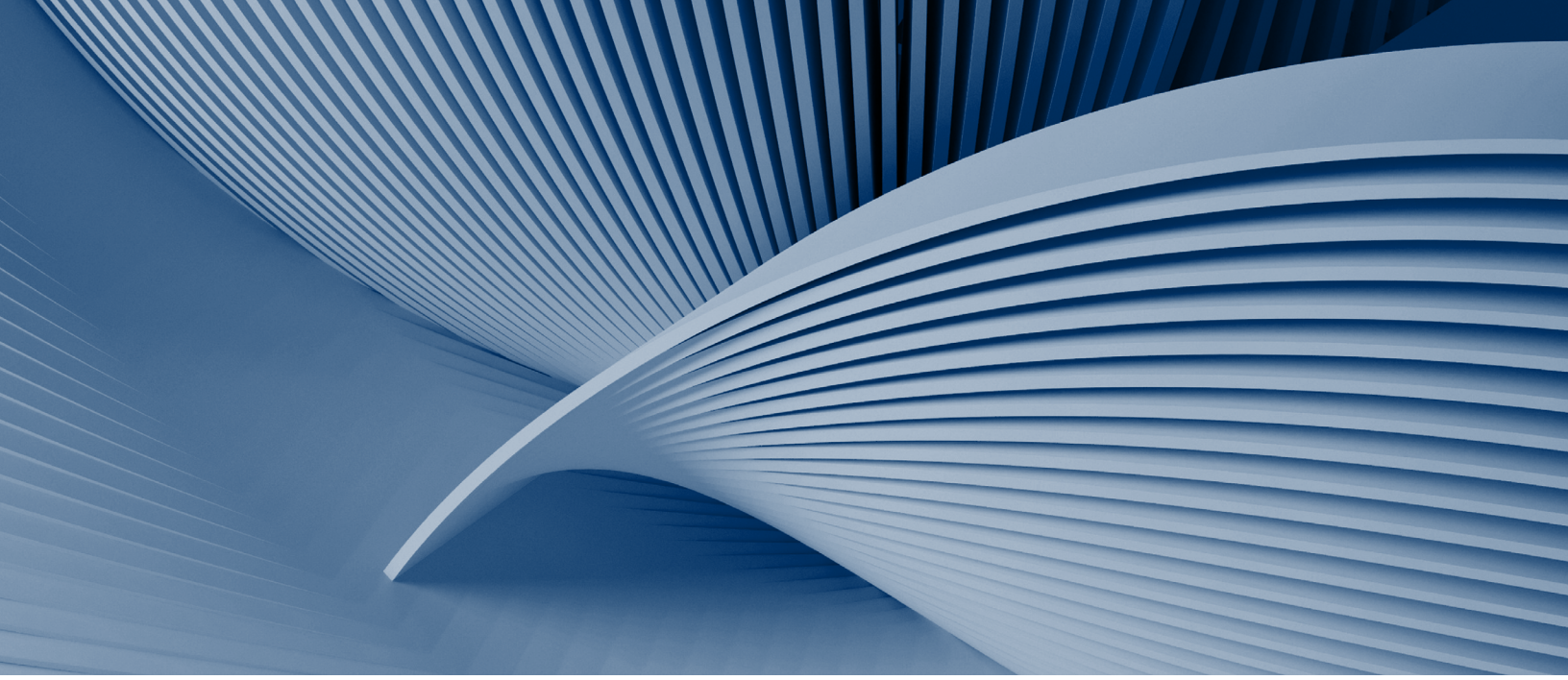
CISOs as Board Directors

CISO Board Readiness Analysis

Table of Contents



SEC Sparks Demand for Cyber-Savvy Board Directors

New SEC rule changes are expected to require public companies to formally disclose the cybersecurity expertise of board members, as well as the board's governance practices in overseeing the cybersecurity risk for the company.

The added transparency resulting from the new SEC rules will provide shareholders with a clear understanding of a board's cybersecurity expertise. On most boards, cyber understanding is insufficient. Recent quantitative research by The CAP Group revealed that 90% of Russell 3000 companies lack even a single board director with cybersecurity expertise.[1]

This highlights the opportunity to remedy this potential skill shortage in 2023 and beyond. In response, many companies will likely be compelled by the market to appoint a board director with proven cybersecurity expertise. CISOs appear to be one logical pool of candidates to fill this gap, but the question arises as to whether CISOs possess the qualifications to serve as effective board members. Additionally, there are questions in the market as to how many credible board-ready CISOs are available for this role.

To address these concerns, IANS Research, Artico Search and The CAP Group collaborated on a research study that evaluated the qualifications of CISOs in companies listed on the Russell 1000 Index, against the characteristics of credible cyber director candidates for corporate boards. These characteristics will be referred to as "board traits" throughout this report.[2]

We sourced this data from publicly available sources, including data from LinkedIn, executive bios, speaking bios, press releases and interviews. We also cross-referenced this data against self-reported information from IANS' and Artico's annual CISO Compensation and Budget study and verified and supplemented it with our firsthand knowledge of the representative sample.[3]

A cross-disciplinary team of cybersecurity experts and data scientists analyzed the data, resulting in a comprehensive study of the board readiness of CISOs across the Russell 1000. This report presents key findings from the study, along with quotes and insights from Steve Martano, a partner and executive recruiter in Artico Search's cyber practice, and Brian Walker, the CEO and cyber board advisor at The CAP Group.

---

[1] Walker, Brian. (2023, Feb. 6) 90% Of Boards Are Not Ready For SEC Cyber Regulations.

[2] The Russell 1000 Index comprises the top 1,000 U.S. public companies by market capitalization.

[3] Given that the research sample of 330 companies is a representative subset of the Russell 1000, the remainder of this report will refer to the sample as the Russell 1000 or R1000.

5 Key Traits for Cyber Experts on Corporate Boards

To determine the essential board traits of a cyber board director, we examined the profiles of CISOs who currently hold corporate directorships.[4] Additionally, we pulled from the expertise of Steve Martano, who has experience in both cyber executive recruiting and board recruiting, and Brian Walker, who has experience as a board director, CIO and CISO, and as an advisor to corporate boards on cybersecurity matters.

Our analysis identified five overarching board traits that companies seek in cyber board director candidates, also listed in FIGURE 1.

Infosec tenure

Deep domain expertise with firsthand experience in cybersecurity is vital for providing a critical eye to the effective management of cybersecurity risk. This core strength allows a director to ask the right questions and challenge assumptions. Tenure as CISO and in cybersecurity were used as key indicators in our analysis.

Broad experience

Effective board directors adopt a holistic view of the business and can connect the dots between functions and risk. Directors with cross-functional experience are better equipped to engage in holistic, strategic board-level discussions because they think about the business holistically, rather than a single function. Prior experience in noncyber roles, such as founder, strategy executive, commercial leader or noncyber strategy consultant, is indicative of this trait.

Scale

Board members must be capable of dealing with organizational complexity and navigating a broad range of stakeholders. The size and global nature of the CISO's current or recent company serve as indicators of this trait.

Advanced education

An advanced degree for board members enhances the board's credibility with external stakeholders and is viewed as indicative of critical thinking and analytical skills. We used relevant advanced degrees in disciplines such as, but not limited to, tech, engineering, business and law as criteria for this trait.

Diversity

Boards are interested in candidates from diverse backgrounds for a variety of reasons including SEC diversity guidelines.[5] Recruitment efforts for board members are able to favor self-identified females and underrepresented minorities. To evaluate this trait, we relied on self-reported data.[6]

"The transition from executive leadership to board directorship is profound, and many struggle to adapt. Our experience shows that these are five of the key traits found in those who are able to successfully move from executive to board director."

– Brian Walker

"Board discussions are distinctly different from executive leadership discussions because boards focus on governance and risk guidance. We identified these five specific traits because to serve as an additive board member, one must bring a unique combination of domain expertise and strategic governance, as well as a pedigree that advances the prestige and diversity of the board makeup. In today's world, boards are seeking diversity of experience and thought, and expanding board opportunities to underrepresented groups."

– Steve Martano

[4] Corporate board experience excludes volunteer boards, advisory boards and boards designed to promote industry standards or company cooperation, as they do not carry the same degree of fiduciary responsibilities as corporate boards.

[5] SEC rule 5605(f) states that as a general requirement, each company must have at least two members of its board of directors who are diverse, including at least one who self-identifies as female and at least one who self-identifies as an underrepresented minority or LGBTQ+.

[6] We validated the diversity metrics against the self-reported data from the annual Compensation and Budget Survey conducted jointly by IANS Research and Artico Search.

FIGURE 1

Preferred Traits for Cyber Corporate Board Directors

Trait	Rationale	Criteria applied
Infosec tenure	Deep domain expertise; able to ask the right questions and challenge assumptions.	5+ years tenure as a CISO and 10+ years tenure in infosec.
Broad experience	A holistic understanding of the business; able to connect the dots and make decisions.	Experience in noncyber functional roles such as a founder, in a strategy role or as a noncyber strategy consultant.
Scale	A global perspective and ability to navigate a wide array of stakeholders.	Experience as the head of infosec in large, global organizations.
Advanced education	Enhanced credibility of the board with external stakeholders.	An advanced degree in tech, engineering, business or law.
Diversity	Brings different perspectives to the table to help the board identify blind spots and meet diversity requirements.	Self-identifies as female or from an underrepresented group.

CISOs on Boards Today Possess These Key Traits

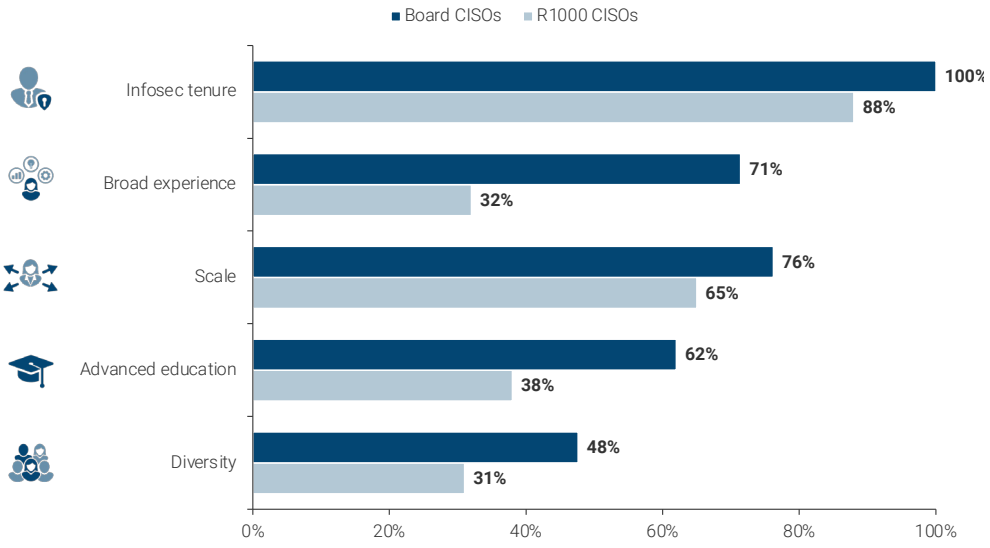
To provide a baseline for our analysis, we identified CISOs who currently hold board positions—aka board CISOs. We then evaluated both the Russell 1000 CISOs at-large and the board CISOs against our board criteria to gauge the overall readiness for board service.

Board CISOs possess more board traits than the average CISO. The most significant difference is in cross-functional expertise, with 71% of board CISOs possessing this trait versus 32% for the R1000 average.

Additionally, board CISOs have notably higher percentages for the advanced education trait and diversity (see FIGURE 2).

FIGURE 2

Board Traits Among Russell 1000 CISOs



"Board seats are coveted, prestigious appointments, so it makes sense that companies appoint directors who are highly educated and whose appointment will look good on a press release."

– Steve Martano

"The data for having a well-rounded background was compelling. Those on boards were over twice as likely to bring a broad perspective to the table with experiences outside of cyber. Rotations in nontechnology roles, or even within IT, can provide a richer appreciation for the complexities in other domains."

– Brian Walker

CISO Readiness for Board Roles Varies Widely

Having identified the key board traits and validated them against board CISOs, we assessed a representative sample of Russell 1000 CISOs to gauge the board readiness of that pool of potential candidates.

Here are the findings, as shown in FIGURES 3 AND 4.

- **14% are ideal candidates,** possessing at least four out of the five board traits. Two-thirds of these CISOs have cross-functional experience and nearly all work at large global firms. They are highly educated and most meet diversity criteria.
- **33% are strong candidates,** meeting three out of the five board traits. Nearly all have served as a CISO for at least five years and have at least a decade of cybersecurity experience. Most have experience dealing with the complexities and scale of large companies, and half have advanced degrees in tech or business. However, they have notably lower percentages for diversity and cross-functional experience than the pool of ideal candidates.
- **52% are emerging candidates,** checking the box on one or two board traits—in most cases, a combination of infosec tenure and scale. This group has far fewer CISOs with cross-functional experience, advanced degrees or diversity criteria.

"Our prior research indicated that 90% of Russell 3000 companies lack at least one director with cyber expertise. This new analysis indicates that, at most, half of Russell 1000 companies could reasonably expect to leverage CISO expertise at the board level. But that still leaves nearly half of Russell 1000 companies searching for board-level cyber expertise."

– Brian Walker

"Our data shows there is a large portion of the population of CISOs who could emerge as board-ready in the next several years. Both boards and CISOs would benefit from aligning on expectations for a board-ready cyber expert, preparing this CISO community aggressively to help meet long-term board needs."

– Steve Martano

FIGURE 3

R1000 CISOs Split Into 3 Groups in Terms of Their Board Readiness

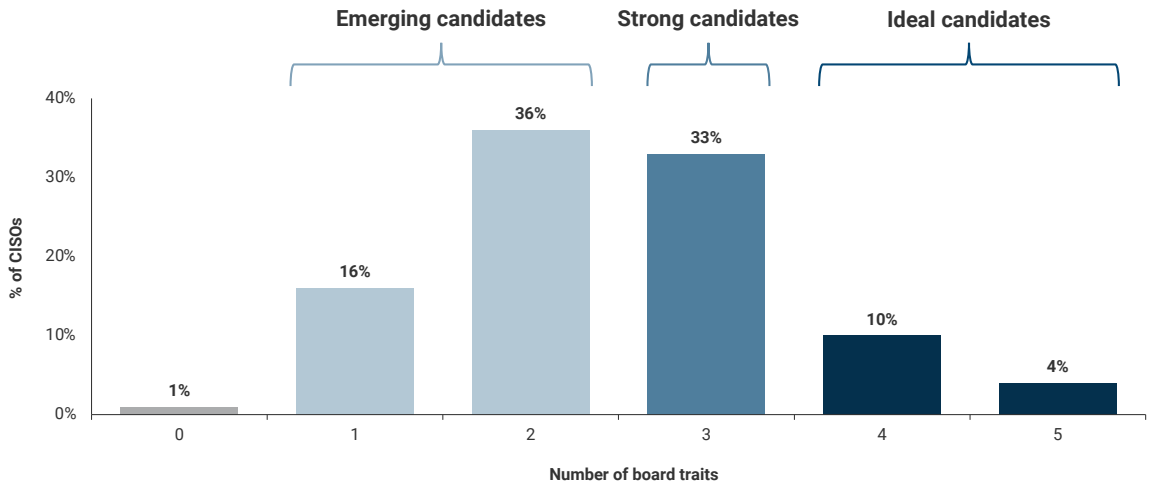
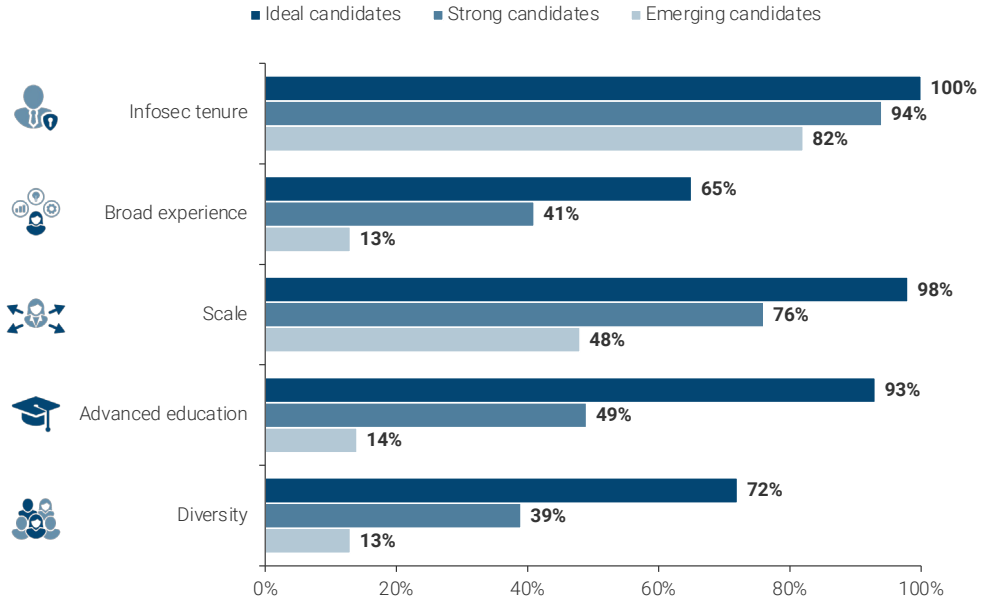


FIGURE 4

The Presence of Board Traits Among the 3 Candidate Groupes



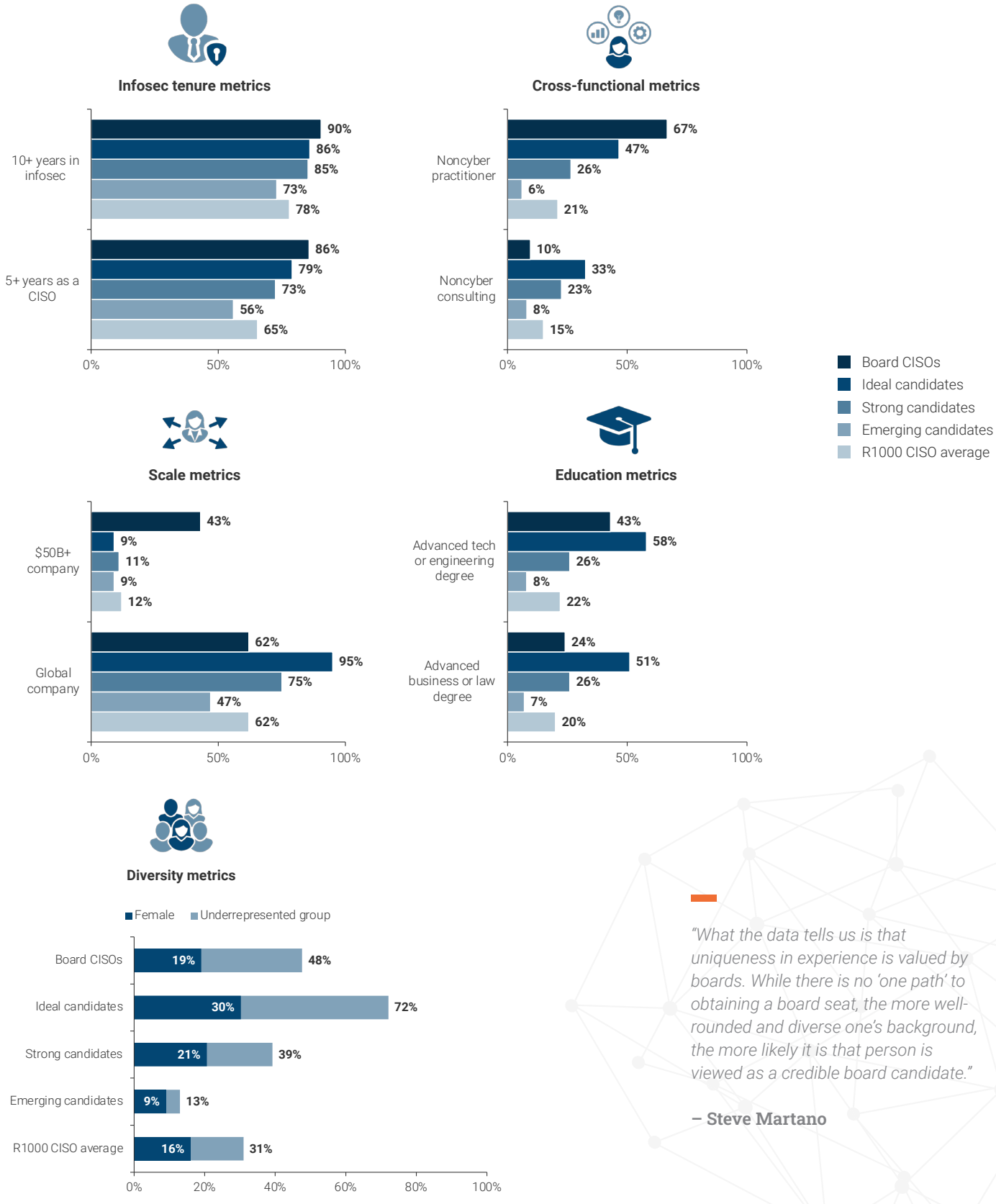
Underlying Metrics Reveal Significant Group Differences

This section provides a closer examination of the metrics that underlie each board trait and highlights the significant differences among the three candidate groups, as well as the group of CISOs who already have board director experience, and the overall Russell 1000 average (see FIGURE 5).

- **The board CISO group demonstrates that possession of all board traits is not required:** For example, a CISO with executive-level experience at a global company exceeding $50 billion in annual revenue, even with less than five years of CISO experience, can be a strong candidate if they have had one or more roles outside of cybersecurity.
- **The ideal candidates outperform board CISOs in some areas, particularly in terms of education and diversity:** Nearly all CISOs in the ideal candidate pool hold a master's degree, split evenly between tech and nontech disciplines. Furthermore, most work at firms with global operations and more than 70% are diverse, with a third identifying as female.
- **The emerging candidates need more time to become well-rounded professionals:** Most CISOs in this group have not pursued higher education, such as an MBA, nor have they gained the experience of working in complex environments found at large global firms. Additionally, their career paths have not extended beyond cybersecurity.
- **There's an "it" factor that no metric can fully capture:** Current corporate board directors with cyber expertise include executives who have served in high-level corporate positions, U.S. presidential administrations and possess advanced degrees from prestigious universities such as ivy league or military academies, as well as other unique backgrounds. In many cases, directors have a unique combination of individual traits, rather than an overwhelming single "superpower."
- **Soft skills are vital:** While our analysis focused on specific, measurable traits, it is important to recognize soft skills determine the success of directors. Boards are close-knit working teams of highly talented and successful people where the conversations are often nuanced; topics are strategic and ephemeral; and collaboration requires clear, on-point discussion. In addition, there is an expectation of a level of polish and gravitas expected in such a setting, something fostered over a career and which does not happen overnight.

FIGURE 5

The Board CISOs Group Displays the Strongest Underlying Metrics



"What the data tells us is that uniqueness in experience is valued by boards. While there is no 'one path' to obtaining a board seat, the more well-rounded and diverse one's background, the more likely it is that person is viewed as a credible board candidate."

– Steve Martano

Most CISOs Have Yet to Embrace Board Certification Programs

Board certification programs that introduce new directors to board governance have been available for years and can provide a valuable jump-start for executives who are ascending to board service. Offerings from the National Association of Corporate Directors, Harvard, Stanford University, Carnegie Mellon University and an increasing number of universities provide a strong set of alternatives for CISOs seeking to bolster both credentials and knowledge as they seek to serve on boards of directors.

However, despite the availability of these programs, only a small percentage of R1000 CISOs have pursued board certification to date.

This trend is consistent among the candidate groups we studied, where just 2% of ideal and 1% of strong candidates have completed a board certification. Notably, board CISOs have a higher certification levels than the average, but this represents only 10% of board CISOs, as shown in FIGURE 6.

While board certification is often considered a desirable credential, our findings suggest it is not yet a critical requirement for CISOs seeking board directorships.

"A certification used only as a credential is of limited value. However, a certification that involves gaining significant knowledge can provide insights that a CISO wouldn't otherwise gain in a day-to-day executive role."

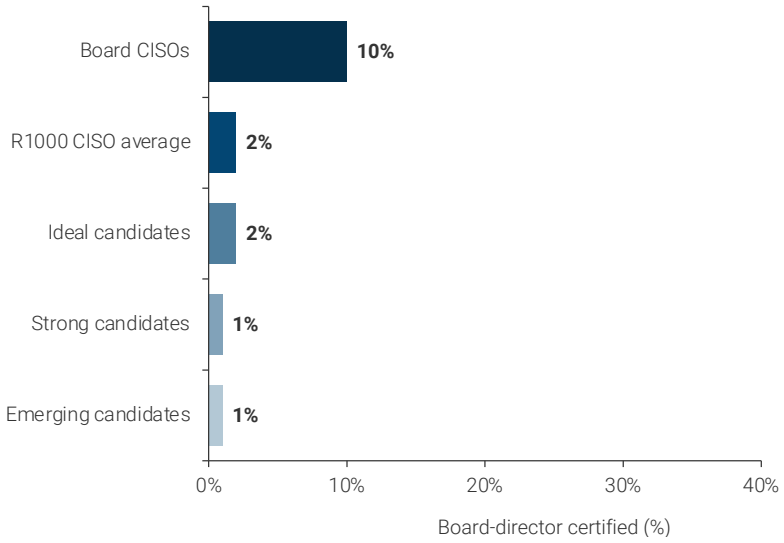
– Brian Walker

"Since there is no consensus on which programs are most effective, not all certificates and programs are viewed equally by the market. Board directors would benefit from guiding CISOs to programs they consider valuable to an additive director. Given limited time and funds, CISOs should seek certification programs with premium, well-established brands, while soliciting feedback from directors in their own network to ascertain which programs are considered top tier."

– Steve Martano

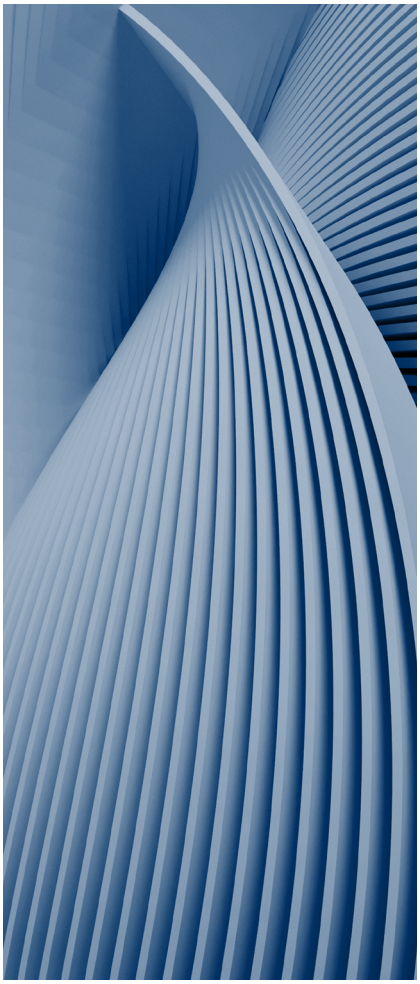
FIGURE 6

Just a Fraction of R1000 CISOs Are Board-Director Certified



Recommendations for Companies Considering CISOs for Board Roles

When it comes to adding cybersecurity expertise to a company's board, there are several options to consider, including engaging outside board-level experts, recruiting existing directors with proven cyber experience, or upskilling current directors with cyber-specific governance skills. However, for companies considering the CISO route, there are key factors to keep in mind:



The Russell 1000 is the right starting point

This is a good starting point for identifying potential CISO candidates. CISOs in the R1000 are likely to have the requisite cybersecurity expertise necessary for a board role. These public companies are far-reaching, diverse and generally report a high level of cyber accountability.

Cast a wide search net

Following the SEC rule change, many companies will launch a search for cyber board candidates. Qualified candidates are scarce, especially those considered ideal, and active CISOs are not likely able to take on multiple board seats. In these conditions, searches should be cast wide and candidates with a variety of profiles should be considered.

Prioritize diversity

If diversity is a key priority for the board, then companies should be prepared to compromise on other requirements, such as nontech expertise or career history at large global companies. Candidates who are diverse will be in high demand and those who possess other qualifications will be even more sought after.

Consider board certification a nice-to-have

While board director certification is a desirable qualification, adoption levels of such programs among CISOs are low. Therefore, companies should consider it a "nice-to-have," rather than a hard requirement for the time being. Companies should also consider offering board program enrollment for newly appointed directors to help them gain the necessary skills or desired accreditations.

Look for the "it" factor

When looking for candidates, it's important to consider the "it" factor by looking for unique qualifications among the shortlisted candidates, including those with diverse backgrounds and experiences that may bring a fresh perspective to the board.

Have a plan B

CISOs are not the only the pool of prospective candidates, and boards may have to wait several years while CISOs in the emerging candidate pool upskill. In the meantime, boards can recruit other business leaders out of cyber companies or other tech leaders less deep in cyber but with enough exposure to be credible.

Recommendations for CISOs Considering Board Roles

For CISOs hoping to pursue roles as cyber experts on corporate boards, we recommend assessing their soft skills, analyzing gaps in their experience and strengthening their career narrative.

Evaluating Soft Skills

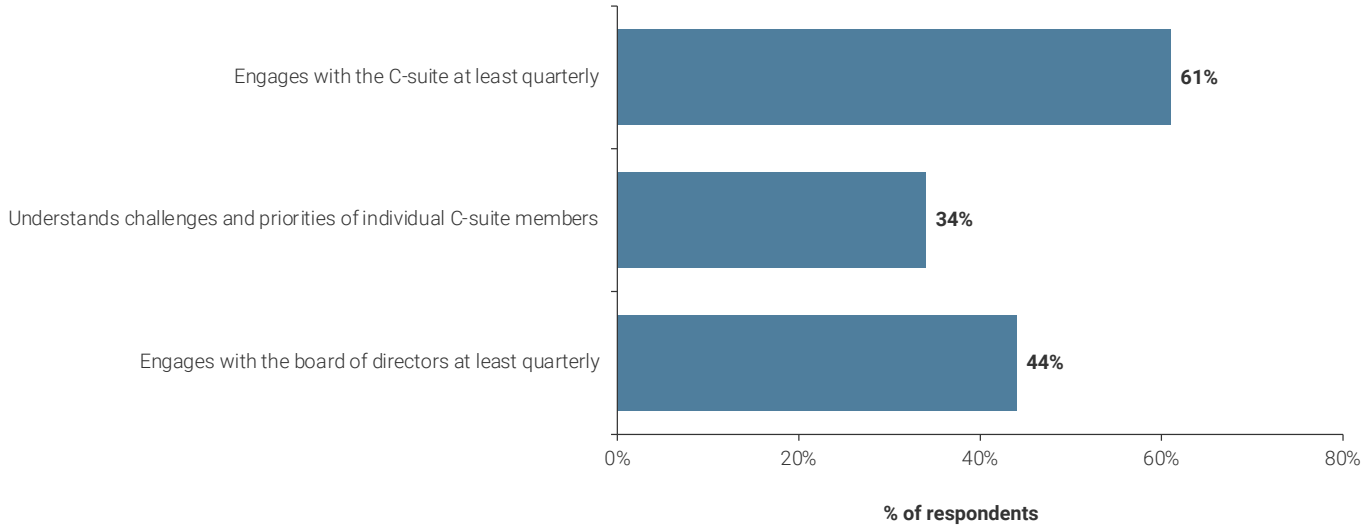
While board traits serve as the hard criteria for shortlisting cyber expert board candidates, soft skills are equally important and assessed in competency-based candidate interviews.

As board directors, CISOs must be capable of providing governance guidance; standing their ground alongside business executives; and demonstrating proficiency in influence, persuasion, empathy, relationship management, active listening and clarity of messaging.

One way for CISOs to gauge their soft skills is by evaluating their relationships with their company's executives and board of directors. CISOs who actively participate in C-suite and board meetings and who have developed a deep understanding of individuals' agendas generally exhibit strong soft skills. However, most CISOs do not fall in that category. A 2023 survey fielded by IANS Research and Artico Search found that 44% of CISOs regularly engage with the C-suite and board and 34% have a solid understanding of the challenges and priorities of individual executives (see FIGURE 7)[8].

FIGURE 7

Gauge Soft Skills From Current Executive-Level Relationships



"Technology and cybersecurity expertise alone are insufficient for board directorships. Board directors operate at a strategic level and, in most boards, there is no room for 'one-trick ponies' because adding a new director for every complex domain of expertise isn't scalable. It follows that CISOs who seek board directorships should bring more to the table in terms of noncyber experiences or diversity, as well as financial acumen and executive presence."

– Brian Walker

[8] Reference to the 2023 CISO Compensation and Budget survey.

Filling in Potential Gaps

For CISOs who need to up-level their board traits and/or soft skills, we recommend a three-tiered improvement plan based on which type of candidate CISOs profile as—emerging, strong or ideal:

Emerging candidates should focus on experience diversification

These CISOs possess fewer than three board traits. Their options to up-level include diversifying their experiences in terms of the industry or global companies, seeking noncyber experiences such as in a strategic or consultative role or by investing in an advanced education like an MBA.

Strong candidates should polish their soft skills

This group possesses three out of five board traits. By investing in their soft skills, financial literacy and executive presence, they will better prepare themselves for new leadership opportunities including board directorships.

Ideal candidates should consider getting board certified

These CISOs possess four or all five board traits. To stand out even more, we recommend they seek out trusted certification programs available to executives interested to join boards such as from National Association of Corporate of Directors and major universities. These programs provide not only valuable credentials, but also help provide valuable knowledge required for board directors that are often not commonly encountered by executives.

"Some CISOs have experience as board members at small nonprofit organizations or serve on one or more advisory boards. For corporate boards, this typically has limited value because these types of board seats do not involve fiduciary responsibilities or corporate governance."

– Steve Martano

Building a Personal Brand

CISOs, though part of a tight-knit community, may not be widely recognized outside of cyber circles. To expand their visibility and exposure, we suggest CISOs focus on:

Keeping an updated LinkedIn profile

CISOs should ensure their LinkedIn profile is complete, up to date and visible to the public. Many CISO profiles we encountered during our research had limited information and were outdated or hidden. A comprehensive profile that highlights your education, certifications and career experiences can help stand out and attract attention.

Crafting a compelling career story

In addition to a standard resume or LinkedIn profile, CISOs should develop a career story that focuses on the key decisions, successes, failures and pivotal moments that shaped their professional journey. It should emphasize the influential people they encountered, including mentors and influencers. Sharing this story through speaking engagements or interviews can help CISOs captivate their audience and differentiate themselves.

Cultivating a diversified network

While it is natural for CISOs to primarily interact with other technical leaders and gravitate toward cyber-focused events, it is vital to diversify their network. Actively seeking relationships with noncyber executives allows CISOs to gain fresh perspectives, expand their reach and build a well-rounded professional network.

By focusing on these areas, CISOs can enhance their personal brand, increase their visibility beyond the cyber community and have a greater impact in their field.

"Be honest and self-aware when assessing your readiness to serve. Solicit coaching from experienced board directors when defining your game plan. The transition to the board is significant, so plan methodically for the long haul."

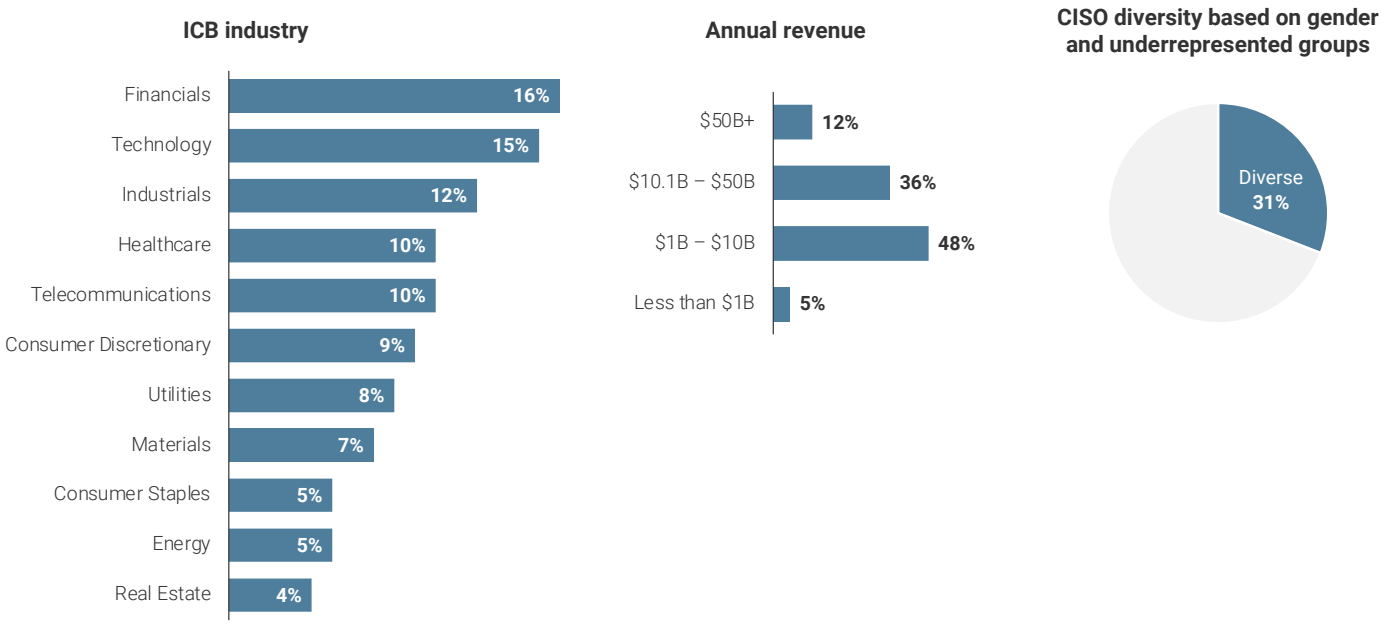
– Brian Walker

Methodology

For this study, we compiled data on a sample of Russell 1000 companies and their current CISOs. The sample size is 330, or one-third of the Russell 1000 list. We selected the sample ensuring the consistency in breakdown of the companies by Industry Classification Benchmark (ICB) and size, as well as by CISO gender and diversity (see FIGURE 8).

FIGURE 8

Russell 1000 sample group breakdown



The data collection sources include LinkedIn, executive bios, speaking bios, press releases, interviews and firsthand knowledge of companies and CISOs.

Data was collected in the month of April 2023 and companies selected were from the 2023 Russell 1000 Index.

About Us

Artico Search

Founded in 2021, Artico Search's team of executive recruiters focuses on a "grow and protect" model, recruiting senior go-to-market and security executives in growth venture, private equity and public companies. Artico's dedicated security practice delivers CISOs and other senior-level information security professionals for a diverse set of clients.

IANS Research

For the security practitioner caught between rapidly evolving threats and demanding executives, IANS Research is a clear-headed resource for making decisions and articulating risk. We provide experience-based security insights for chief information security officers and their teams. The core of our value comes from the IANS Faculty, a network of seasoned practitioners. We support client decisions and executive communications with Ask-an-Expert inquiries, our peer community, deployment-focused reports, tools and templates, and consulting.

The CAP Group

The CAP Group advises board directors and officers seeking pragmatic advice on cyber-risk matters. Founded in 2017 and based in Dallas, the firm supports clients ranging in size from global Fortune 500 to regional G2000. The CAP Group brings decades of practical experience in the management of cyber-risk and understands the unique needs of both the board and executive leaders. The CAP Group's advice focuses on ensuring transparency and collaboration between the board and the executive team, providing the insights required to provide effective shareholder risk management.