NIGHTDRAGON Diligent Institute

STATE OF CYBER AWARENESS IN THE BOARD ROOM REPORT

An In-Depth Analysis of the State of Cyber Awareness, Education, and Expertise of Board of Directors at S&P 500 Companies

Endorsed by Industry Leaders, Including:

NIGHTDRAGON Diligent Institute Diligent NYSE SpencerStuart ISC2 GLASS LEWIS Moody's

Foreword

After more than 20 years in the cybersecurity industry and assisting with more than 5,000 incidents as a four-time CEO, as well as a member and advisor of many boards of directors, it's clear the speed and scale of digital attacks today have intensified into an existential crisis for our current world order. In 2022, over 422 million individuals were affected by cyberattacks in the United States alone, with each attack on a business costing an estimated $4.45 million on average. And by 2025, cumulative losses are expected to top $10.5 trillion.

And yet, despite this rising risk targeting businesses of every size and industry, there remains a large gap at the highest levels of many of our nation's largest organizations when it comes to cyber literacy and education. In conjunction with leading industry partners, we sought to measure just how large this gap is and determine the prevalence of specialized cybersecurity and technology skills among corporate directors of S&P 500 companies.

In the "State of Cyber Awareness in the Board Room Report", NightDragon and Diligent conducted a thorough review of the members of the boards of directors of the S&P 500, an index of the largest companies listed on stock exchanges in the United States. This report and its findings are endorsed by leading industry organizations, including the New York Stock Exchange, Glass Lewis, ISC2, Spencer Stuart, and Moody's. By joining together to release and endorse this report, we are united in our hope to advance cyber education and expertise at all levels of the organization, including the board of directors.

Our research confirms that, despite the rising risk and cost of cyberattacks, 88% of S&P 500 companies do not currently have an executive with specialized cybersecurity experience on their board to guide them on risk mitigation efforts, and 57% lack similar specialized experience in other technology categories. Boards have a direct responsibility to shareholders to mitigate risk to the organization, yet, as the data shows, many do not possess the background, education, or training to fluently "speak the language of cybersecurity" and adequately combat cyber risk.

Similar to how the Enron and Worldcom scandals forced even the most responsible businesses to put more robust financial compliance measures in place, every corporate board risks falling short in their duty to shareholders if they don't take this threat of cyberattacks seriously. As someone who has served as a board director for over 40 companies, including Delta Airlines, Five9, and more, I've seen first-hand the impact an industry expert or educated board can have on interpreting cybersecurity posture and helping to guide future strategy in a way that will drive long-term success for the business.

The good news is momentum is moving in the right direction. Companies are realizing they can no longer ignore the issue, nor can they treat security as just some ancillary function that's separate from the rest of the operations. And, as the federal government gets more heavily involved in cyber policy and regulation, including for incident reporting or requirements to meet certain standards, we're seeing more corporations take action to educate their boards more proactively and have security teams reporting regularly to the board.

The time to act is now because the situation is only going to get worse. Don't wait to get hacked to find out if you have the right skills. It takes a village in cybersecurity, and we need a bigger, stronger and more educated village if we want to thrive in our new cyber and digital world order.

Dave DeWalt
Founder and CEO of NightDragon
Former CEO of FireEye, McAfee and Documentum
Board Member of many organizations, including
Delta Airlines and Five9

Table of Contents

Introduction

Businesses are spending more money every year trying to defend their digital environment from attackers. In fact, as other areas of the business face tighter budgets this year, 48% of CEOs planned to increase investment in cybersecurity and data privacy, according to a survey from advisory firm PricewaterhouseCoopers. Meanwhile, cybersecurity remains the most challenging area of oversight for corporate leaders, according to a recent survey of public company directors by Diligent Institute and Corporate Board Member.

There's a good reason for that. It's clear the digital revolution is only gaining steam, increasing the risk surface every day for attackers to target. Technology now underpins every aspect of our lives and any threat to that digital infrastructure could mean major disruptions for millions of people - if not more catastrophic consequences.

We're already beginning to see the impacts of this on our personal and corporate lives, including attacks targeting financial organizations, hospitals, critical infrastructure and more. As previously mentioned, these attacks culminate in estimated global losses of around $10.5 trillion by 2025, as well as drive further ramifications to ongoing operations and business reputation.

As a result, cybersecurity is increasingly becoming a discussion at the board level and part of the overall company compliance and risk strategy. And now, as AI and other new innovations are poised to only further amplify the power of cyber incidents, the federal government is getting involved. The Biden administration is in the midst of mandating that companies quickly disclose breaches and publicize risk mitigation strategies as part of its annual regulatory reporting requirements and the U.S. Securities and Exchange Commission has adopted new regulations around the topic, among other efforts.

With so much at stake, NightDragon and Diligent analyzed the leadership composition of the Boards of the S&P 500, with a goal to determine if there was a potential gap in education and expertise at the nation's largest and most influential companies when it comes to mitigating cyber risk and guiding strategies from the top down. The report and its findings are endorsed by industry leaders including the New York Stock Exchange, Glass Lewis, ISC2, Spencer Stuart and Moody's.

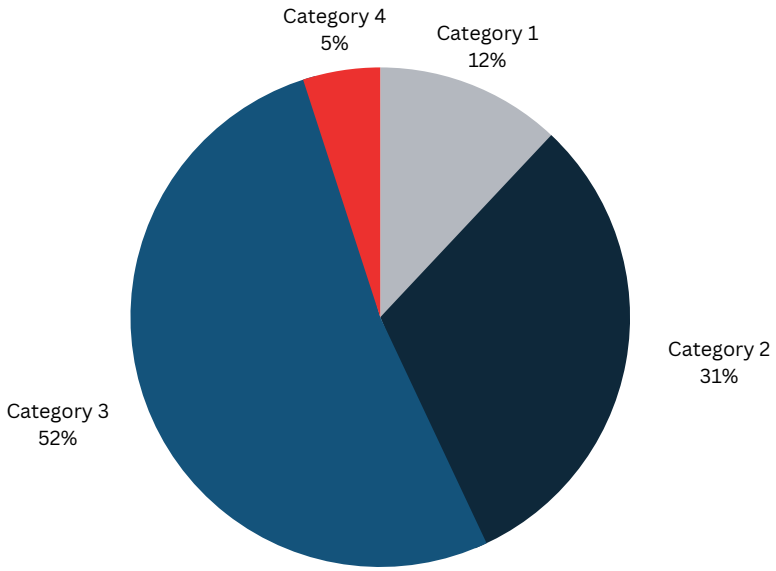
"The reality is that cybersecurity is a growing risk across all industries and businesses. Boards of directors have a growing responsibility to build their competency around cyber risk so they can implement more effective governance strategies and have more meaningful conversations with management."

- Brian Stafford, President and CEO of Diligent

Findings

NightDragon and Diligent undertook a thorough study of all S&P 500 organizations, the members of their Boards of Directors and their backgrounds.

While previous role experience is not the only measure of expertise on the topic of cybersecurity, these findings show that there is room to grow for Boards of Directors when it comes to educating themselves and incorporating the right expertise as part of their overall governance strategies.



12%

CATEGORY 1: Companies that have at least one current or former "cyber expert" on the board. These individuals may include:

- Current or former Chief Information Security Officer (CISO)
- Current or former Chief Information Officer (CIO) of a company that offers cybersecurity services
- Current or former CEO of a company that offers cybersecurity services

Only seven businesses have a current or former Chief Information Security Officer (CISO) on their board (1.4% of the S&P 500), with one CISO serving on two S&P 500 company boards. None featured their own organization's CISO sitting directly on the board, even if the CISO may present to the board at some regular cadence.

31%

CATEGORY 2: Companies that had technology expertise on their board, but not necessarily a cybersecurity specialist. These individuals are likely informed on cybersecurity and overall technology topics but are less direct experts on the topic than those who fall into the preceding category. These individuals may include:

- Current or former CIOs of companies that do not offer cybersecurity services
- Chief Technology Officers
- Senior Vice Presidents of IT
- Someone with a connection to the cyber world who served in a current or former C-suite (except CEOs of cyber- security companies, who were included in Category 1)

52%

CATEGORY 3: Companies that have at least one board member with some adjacent connection to the cyber world, but no direct previous experience in a practitioner cybersecurity or technology role. That would include any of the following:

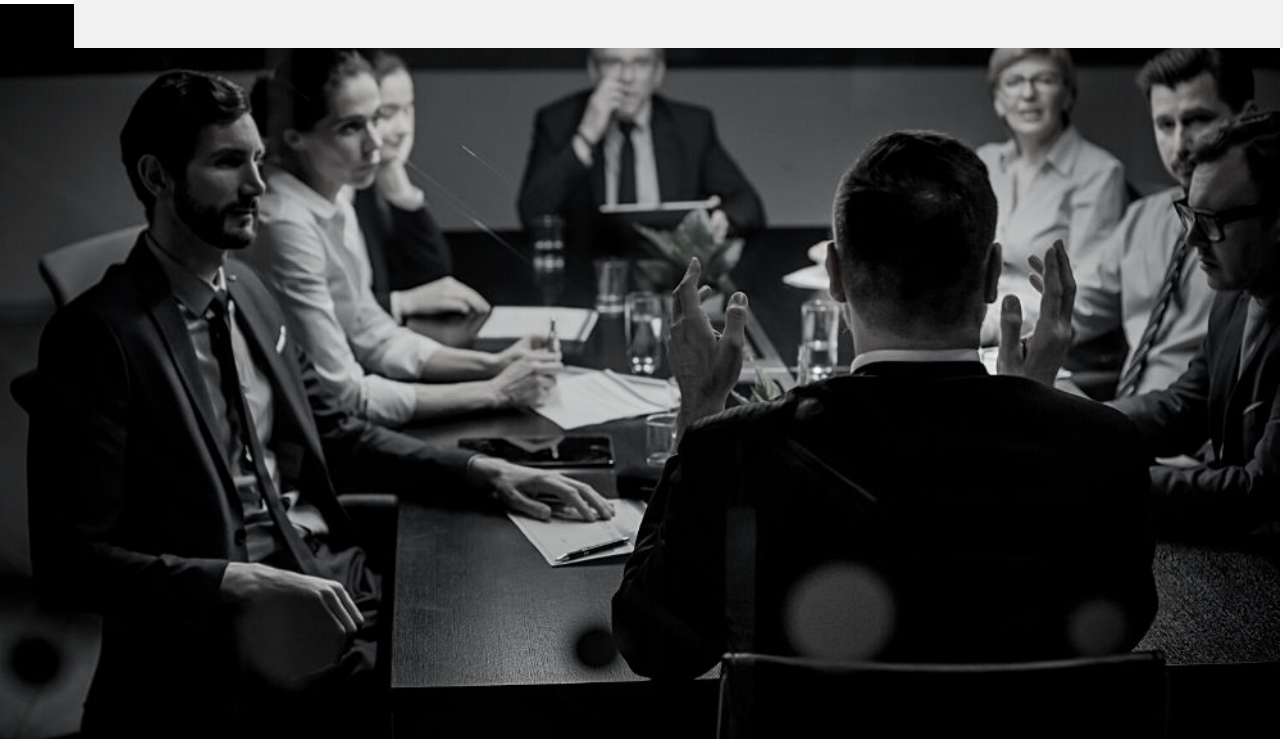
- Board member who has served on the board of another IT/ cyber industry company
- Board member who has completed cyber education, belongs to cyber associations or committees, or has some other cyber affiliation
- Board member with some tech and/or IT experience, but not in a C-level role, and not specific to cybersecurity

5%

CATEGORY 4: Companies that do not meet any of the above criteria.

"Cyber risk is now one of the top risk areas boards are spending time on and raising their awareness of the resiliency needs across their respective organizations and sectors. With the recent finalization of the SEC rules on cybersecurity disclosures, I am expecting the evolution to continue at a rapid rate."

- Myrna Soto, Board Member, CMS Energy Corporation, TriNet, Spirit Airlines



A Bright Spot for Gender Equity

According to the 2023 U.S. Spencer Stuart Board Index, 33% of all S&P 500 board directors are women overall. Yet, cybersecurity expertise represented a bright spot for gender equity in the board room. Four out of the six CISOs that currently serve on S&P 500 boards are women, according to Diligent data.

Perspective From Board Leaders

"It's hard to gloss over cyber risk when you are looking in the eye of a fellow director with cyber operational experiences. It is important, however, that all board members be curious and have the confidence to ask questions about the cyber risks and mitigations. My most satisfying moments in the boardroom have been when other directors ask great questions in cyber discussions. The only stupid cyber questions are those left unasked."

– Admiral Jan Tighe, Board Member, Goldman Sachs

"I still observe a gap in the understanding of what a cyber threat truly entails and how it can be effectively governed. While boards comprehend the concept of data breaches, the intricate technical aspects often exceed their expertise. Cyber risks are complex and highly technical, so while boards certainly possess greater awareness and good intentions, they still have a long way to go in fully grasping the real-world business impact and effectively mitigating such risks. "

- Emily Heath, Board Member, Gen Digital

"It is imperative that CISOs prepare themselves to broaden their experience level, increase their communication skills in business terms, and become broader than a siloed subject matter expert to become exemplary candidates for the boardroom."

- Myrna Soto, Board Member, CMS Energy Corporation, TriNet, Spirit Airlines

NIGHTDRAGON Diligent Institute

An Eye Towards AI

While cyber threats continue to rise, we are also in the midst of another digital revolution: the rise of a new Era of Artificial Intelligence (AI). This is a consequential period of technology innovation that promises to open up a new frontier of possibilities and spur life-changing discoveries that could alter most, if not all facets of our lives.

Businesses everywhere are rushing to figure out how they can incorporate this technology, including leveraging the advantages of automation, predictive analytics, large language models, and other emerging technologies to win against rivals. More than 90% of NightDragon's advisory panel, made up of nearly 80 CISOs and related roles, believe implementing an AI strategy is imperative for their company's future success.

These same conversations are escalating to the boardroom. According to a recent study by the Diligent Institute and Corporate Board Member, 51% of directors say they have discussed AI more frequently and in more detail over the past year. Additionally, 31% said they are seeking education on the benefits and risks of AI and 75% see AI playing a role in the boardroom in the future.

While the rise of AI brings immense potential, new efficiencies and innovation capabilities to businesses of all sizes and in every industry, it also introduces new risks. Just like business leaders are rushing to embrace AI, bad actors are already tapping the same technology to get better at infiltrating corporate IT systems. What's more, the addition of new technology further increases the attack surface within organizations. In fact, 100% of our advisory panel believes there will be an increase in cyberattacks against generative AI tools.

The introduction of new technologies like AI further underscores the need for boards to get educated on cybersecurity as a strong foundation for future emerging technology. Innovation is already coming at us at record speed and the urgency for businesses to adopt these powerful new applications is only mounting. At the same time, companies are more at risk of a breach that could impact the brand's reputation, result in a large fine, and potentially jeopardize an enterpriseís whole digital strategy.

The only way to mount a proper defense is to embed cybersecurity into the foundation of everything the company does. And the only way to do that is to make sure that leaders all the way up to the Board of Directors are enabled with the right skills to call the shots.

What's the Solution?

The good news is that more and more boards are looking to add cyber expertise to their ranks, or increase education amongst existing board members. For example, Spencer Stuart's latest annual survey of nominating/governance committee chairs, conducted in the first quarter of 2023, shows an increase in respondents seeking cyber expertise (19% up from 8% in 2022). Additionally, 60% of respondents cited cybersecurity as a topic that would be beneficial toward director development, training and education.

There are several steps that organizations can take to advance the state of cyber awareness at the board of directors' level. Some considerations could include:

1. MAKE EDUCATION A PRIORITY

Companies should seek to educate their existing board members on cybersecurity so directors can start to understand the threat landscape, new technology categories, and be enabled to make informed decisions about risk to the organization. There are many ways to do this. For example, some CISOs will do quarterly "brown bag" lunch meetings, where a different cyber topic is discussed in detail at each. Enrolling their board in cyber certification programs could be another way to go.

2. REGULAR BOARD REPORTING

Companies need to ensure that the CISO or leader of the security team is reporting to the board on a regular basis on the state of business and its risk mitigation efforts. In those briefings - which should happen quarterly, if not more often - the CISO should provide an overview of the company's current risk profile, as well as insight into recent threats that may or may not ultimately affect the organization.

3. INTEGRATED INTO COMPANY STRATEGY

While cybersecurity should be a fixture in the company's regular reporting schedule, board directors should also consider how it can be tightly integrated into every piece of the company strategy on an ongoing basis.

---

4. PRACTICE, PRACTICE, PRACTICE

While we always want to hope for the best, we should also prepare for the worst - no matter the makeup of the board. In addition to being a regular fixture on the company's reporting schedule, boards should also consider what steps they would need to take if a cyber incident were to occur and if those relationships are in place across the business to make informed decisions quickly in a time of need. This could include tabletop exercises, where incident response is practiced, like a fire drill.

---

5. ADD CYBER EXPERTISE DIRECTLY TO BOARD

While education can go a long way to close the gap around cybersecurity, businesses can also consider if adding a CISO to the board directly makes sense for their needs. There are many former CISOs or former cybersecurity leaders now looking to sit on or advise boards, as well as a business' own CISO.

---

6. BUILD A VILLAGE

It takes a village to combat today's cyber threats and no business should have to face this threat alone. Boards should consider how they can work together with others in their industry or broader business community to share best practices around cybersecurity, as well as how they can work in public-private partnership with government organizations.

"Boards are beginning to take action on how they can more effectively help their organizations manage cybersecurity risk. We are seeing boards more proactively educating themselves on cybersecurity, increasing engagement with technology and cybersecurity leaders, and seeking new directors with technical experience to strengthen their oversight capabilities.

However, this will remain a gradual evolution, considering low boardroom turnover. Data from our U.S. Spencer Stuart Board Index supports NightDragon and Diligent's findings: few S&P 500 companies are adding true cyber/tech expertise to their boards. Only 4% of new S&P 500 directors in each of the past three years have true cyber experience."

- Kate Hannon, member of Spencer Stuart's global Technology Officer Practice and head of the firm's Cybersecurity Practice.

How CISOs Can Prepare to Talk to the Board

While boards have a responsibility to escalate their education and effort around cybersecurity, it is important for CISOs to also understand their increasing role in educating the board. This may take some additional preparation on the part of the CISO to ensure that their key messages are hitting home, particularly if the concepts are particularly technical or complicated.

1. DETERMINE THE RIGHT LEVEL OF INFORMATION

While a CISO is on the front lines of defending the organization every day and implementing the latest technology, that doesn't mean that a quarterly presentation to the board should be a 100-slide presentation on the state of the business. CISOs should take time to understand the right level of information to present to the board based on their role and responsibility in overseeing corporate activities and performance, as well as their technical level of education, as they determine what information is most valuable to share.

2. DON'T ALWAYS LEAD WITH CYBER

While CISOs are certainly expected to be well-versed in cybersecurity and technology, the board is all about business risk. CISOs must approach every discussion and potential problem not just from the mindset of a skilled practitioner, but as someone who intimately understands the unique nature of their organization and how security fits in most effectively. That means ditching the industry lingo and always speaking in terms of risk to the business, such as how cybersecurity risk could impact revenue acceleration, international expansion, and other strategic topics.

3. EMBRACE THE REAL WORLD

While cybersecurity should be a fixture in the company's regular reporting schedule, board directors should also consider how it can be tightly integrated into every piece of the company strategy on an ongoing basis.

4. BUILD TRUST BY ASSISTING IN EDUCATION

CISOs can play an important role in educating the board to increase their overall understanding of cyber risk concepts. This can include educating the board on the latest cybersecurity technologies available to the business, how attacks hitting headlines could impact the organization, or evolving market trends. Ultimately, this will help the CISO build further trust with the board and enable the board to make better cybersecurity decisions through a deeper understanding of the industry and trends.

Resources Available

There are many resources already available to companies looking to advance the state of cyber education and experience at the board of directors level. Here are some examples:

Diligent Institute informs, educates, and connects leaders to champion governance excellence. We provide original, cutting-edge research on the most pressing issues in corporate governance; certifications and educational programs that equip leaders with the knowledge and credentials needed to guide their organizations through existential challenges; peer networks that convene directors and corporate executives to share best practices and insights; and awards and recognition programs that celebrate governance excellence. Our current offerings include certificate programs for corporate directors and executives to better understand and oversee both cyber risk and the ethics of AI. Learn more at diligentinstitute.com

The New York Stock Exchange is the world's largest stock exchange, with a remarkable community of 2,400 listed companies and a storied history dating back to 1792. The NYSE is part of Intercontinental Exchange, a leading global provider of data, technology and market infrastructure. The exchange provides listed companies with access to Diligent software to access insights across governance, risk, compliance, audit and ESG.

It also operates the NYSE's own Board Advisory Council, comprising CEOs from some of the world's largest and most well-known companies. Founded in 2019, the BAC hosts networking events to connect diverse board-ready candidates with companies looking to build inclusive leadership on their boards.

Spencer Stuart is a leader in helping corporate boards both evaluate their cybersecurity acumen and proactively appoint new board members with true subject-matter expertise. Based on our experience, we have published several articles to help boards make informed decisions as they aim to build up their overall knowledge of cybersecurity and consider adding directors with technology and cybersecurity expertise.

- Cybersecurity and the Board
- Defining the New Technology Leaders: Winning in a digital world with focused specialization

ISC2 is the world's leading member organization for cybersecurity professionals. Best known for the CISSP certification, ISC2 has more than 500,000 members, candidates and associates around the globe. ISC2 understands the need for board literacy and has developed two certificates to help cybersecurity professionals communicate with the board including:

- Introduction to NIST Cybersecurity Framework (2 CPE credits)
- Gaining Support for Your Security Program (2 CPE credits)

ISC2's entry-level certification, Certified in Cybersecurity (CC), provides you with the foundational cyber knowledge, skills and abilities. With the CC exam and training being offered for free currently, it is an opportunity for board members with minimal cybersecurity experience to understand the basics of the field. Recently, ISC2 hosted a webinar on Board Level Metrics - Getting the Conversation Right, which discussed how to clarify an organization's risk profile in clear and meaningful terms to the board. Additional offerings supporting board education will go to market shortly.

Report by:

NIGHTDRAGON Diligent Institute

Endorsed by:

ISC2 NYSE Moody's

GLASS LEWIS Diligent SpencerStuart

Media Contacts

NightDragon
Sarah Kuranda Vallone, VP Marketing
sarah@nightdragon.com

Diligent Institute
Kelly Blum, Senior Director
kblum@diligent.com