MS CRS 2022 Capstone **Bethany Mayer**

Mentor: Randy Milch **May 9th, 2022**

Is a Cybersecurity Expert Needed on Public Company Boards Today?

Executive Summary

According to the 2021 Cyber Threat Report by SonicWall, there is a 62% increase in ransomware since 2019.[1] There have been 304 million ransomware attacks, 51.1 million crypto jacking attacks, and 32.2 million IOT malware attacks since the beginning of 2021.[2] The global cost of cybercrime peaked at $6.6T USD[3] at the end of 2021. The sophistication of attacks such as the SolarWinds and Microsoft attack, the massive fallout from those attacks in terms of potential loss of IP, personal information and money, and the fact that many of the attacks are being perpetrated by nation states with almost unlimited capital means that public and private companies alike face risk unlike any in the past. The rise in attacks combined with escalating damage make a compelling case that cataclysmic occurrences are likely and could irreparably damage the US economy or even our way of life. The SEC and the White House as well as Congress are putting in place more requirements around specific actions and disclosures the board must take to remain in compliance and avoid a potential investigation and subsequent enforcement action. Given the escalation of cybersecurity attacks, the severity of those attacks, and potential liabilities for both the board and the company, a cybersecurity expert on public boards seems as important now as a "financial expert" on boards was after the Enron debacle. There are many parallels in the level of threat not only to individual corporations, but to the economy and the public markets between the financial risks of the early 2000s and the cybersecurity risks that we face today.

The logic for a cybersecurity expert is that most board members today have neither a technical nor governance-based understanding of cybersecurity. It is difficult for the average board member to ask questions or understand the answers on cybersecurity practice in a company. In a 2019 survey of Fortune 100 companies less than 33% of CIOs believed the board understood cybersecurity information without a cybersecurity expert and less than 40% believed their board communications were effective.[4] In many cases, the CISO is having a one-way monologue with audit committee members who for the most part are financial experts, not cybersecurity experts.

A cybersecurity expert on boards is currently quite controversial. There are concerns about the narrowness of focus an individual with that background might have and given how few seats there are on a board, filling one of the seats with a single topic expert may not provide enough value for the full board or company. It is important to remember that prior to SOX, having a "financial expert" on the board was also controversial for the same reasons. And even as boards are expanding their skills sets today there is discussion about narrowness of knowledge of CHROs, CMOs, and others who were not a

[1] SonicWall Cyber Threat Report, 2021
[2] SonicWall Cyber Threat Report, 2021
[3] https://www.upguard.com/blog/cost-of-data-breach
[4] https://www.marcumllp.com/insights/adding-a-cybersecurity-expert-to-the-board-of-directors

CEO. And yet, given the level of risk and the amount of scrutiny and liabilities possible, having an individual on the board who understands in depth what the company should do to lower cyber risk is prudent and may be required. Beyond having a cybersecurity expert on the board, having cybersecurity addressed in audit may be a sub-optimal committee to have a thorough dialogue on cyber risk.

This paper will attempt to answer the following questions: What are the pressures boards are facing to lower cybersecurity risk? Are boards structured correctly to oversee cybersecurity? What do boards think about the importance of cybersecurity? Is a cybersecurity expert needed on boards to appropriately oversee cybersecurity? If it is a necessity what would the optimum profile of a cybersecurity expert be?

Federal Scrutiny and Oversight of Public Companies Cybersecurity Disclosures and Preparedness are Growing

Over the course of 2020 and 2021, the Office of the President of the US, Congress, the SEC, and Courts have stepped up the scrutiny, enforcement, and requirements for public company boards on areas such as: disclosures, policies, processes, governance, and oversight of cybersecurity. This increased focus by the federal government is a direct result of the massive increase in cybersecurity attacks and the damage of those attacks on public and private companies as well as other entities.

In May 2021 the Office of the President issued a directive entitled Executive Order on Improving the Nation's Cybersecurity[5]. This order was in response to the numerous and egregious attacks that had been escalating over the past several years and came to a head with a massive software supply chain attack using SolarWinds Orion network management software updates to target 18,000 of SolarWinds' customers.[6] One of those customers included the federal government who had deployed the software throughout its agencies. This attack in combination with startling ransomware attacks, such as an attack on Colonial Pipeline and JBS meats, along with several targets throughout the US, created enough concern by the Executive branch to take an active role in establishing more federal oversight and cooperation with private sector companies as well as provide more direction to Federal agencies and their contractors regarding prevention, detection, and mitigation of attacks.

The Executive Order was this President's first address regarding cybersecurity in both private and public settings and helped establish more momentum for the Cybersecurity and Infrastructure Security Agency (CISA) and their work with private sector companies to share more information about potential threats and vulnerabilities as well as provide guidance for companies on cybersecurity policy and planning.[7] This EO by the President made a very strong statement to both private sector US companies as well as other nations, that the US would use its federal authority to combat cybersecurity attacks. Along with Executive Office focus on cybersecurity, the SEC has made cybersecurity a high priority. The SEC charter is to assure transparency and disclosure for all risks and material issues that affect publicly traded companies and financial institutions on behalf of investors. In the case of financial institutions, it has an added focus on safeguarding investor information. As such, the SEC provided guidance in 2018 in the

[5] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[6] https://www.sans.org/blog/what-you-need-to-know-about-the-SolarWinds-supply-chain-attack/

[7] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Commission Statement and Guidance on Public Company Cybersecurity Disclosures.[8] The 2018 guidance had three key elements:

1. Disclosure and materiality: The company should disclose material cybersecurity risks and incidents in managements discussions of financial conditions, descriptions of the company's operations and legal proceedings. Materiality is determined by whether a risk or incident would affect a reasonable investor's view of the company.
2. Board risk governance: The company should disclose the role of the board in the oversight of cybersecurity risk and policies and procedures to allow investors a view of how engaged the board is in this area.
3. Disclosure controls and procedures: The company should disclose how information regarding cybersecurity is gathered processed and escalated to management and the board in a timely manner to allow those individuals to respond to the information. These controls should be reviewed for adequacy when filing any information related to CFO or CEO decisions or documents.[9]

Gary Gensler, the SEC Commissioner since April 14, 2021, acted on 2018 SEC guidance on disclosures regarding cybersecurity. Gensler and the SEC utilized the 2018 guidance to enforce actions against several companies for disclosure violations. Two that are well known are the SEC enforcement action against title insurer First American Corporation and education publisher Pearson PLC. In the case of First American, the company was charged with failure to maintain adequate cybersecurity controls primarily due to the failure of individuals in IT to notify executive management that a vulnerability was present that could cause the exposure of 800 million images of titles and escrows which contained personal information of thousands of customers. A breach did not occur, and as such customer data remained private. However, the company filed periodic reports that did not reflect the vulnerability because executive management was not informed that it was present. When executive management was notified, it was immediately remediated, but because executive management and the board filed previous reports that did not reflect the vulnerability (because it was not known by executive management at the time), and did not have proper controls in place to assure escalation of potential risks, the SEC charged the company and they paid $457K in fines.[10] The key failure of First American was lack of controls which resulted in incorrect disclosures. The SEC also charged and fined Pearson PLC with misleading investors and failure to maintain adequate disclosure policies and procedures following a cybersecurity incident.[11]

What is clear from these actions and the continued actions the SEC is taking against others, is that the SEC is focused on ensuring that public companies provide accurate and timely disclosure of both risks and incidents, and that failure to put in place adequate controls to assure that executive management and the board are informed in a timely manner will be punished. The SEC has taken this stance due to the heightened risk that cybersecurity poses to companies and their stakeholders. It is not enough for

[8] https://www.sec.gov/rules/interp/2018/33-10459.pdf
[9] https://www.skadden.com/insights/publications/2018/02/sec-issues-interpretive-guidance
[10] https://corpgov.law.harvard.edu/2021/08/11/early-sec-enforcement-trends-from-chairman-genslers-first-100-days/

[11] Sullivan and Cromwell memo, August 18, 2021, SEC Charges Issuer with Misleading Investors About Cybersecurity Incident and for Inadequate Disclosure Controls

executive management and the board to be passive in its cybersecurity oversight – as noted by the First American case in which executive management when notified reacted immediately. Executive management and the board must be proactive and must assure that controls and procedures are in place and are being followed by employees at all levels. Although the SEC has focused on disclosure compliance at this time, the next step for the SEC is likely a requirement for additional skill sets on the board that can understand cybersecurity in some depth. Having the skills and competencies to pro-actively govern is the judicial standard. Asking questions isn't good enough, directors need to understand the answers.[12] According to former SEC Commissioner Luis Aguilar, the demands on boards for action on cybersecurity is only going to increase in the future.[13]

Congressional Actions

S808 is a bill introduced in the US Senate on March 17, 2021, by Senators Jack Reed, Susan Collins, Mark Warner, Kevin Cramer, Catherine Cortez Masto, Ron Wyden. The bill is focused on "promoting transparency in oversight of cybersecurity risks at publicly traded companies"[14]. It is also cited as "The Cybersecurity Disclosures Act of 2021". The act requires the SEC to make a rule that publicly traded companies must disclose in their annual reports – either the 10K or the Proxy Statement – the list of individuals who are considered cybersecurity experts on the board. It also requires the board to state why the individuals have the expertise by listing qualifications and authorizes the SEC to create a list of qualifications following some framework such as NIST.[15] In addition, if the company cannot identify a cybersecurity expert the company must identify what other cybersecurity aspects were considered when nominating individuals to the board. As recently as February 8th, 2022, the five Senators backing S808 wrote a letter to Gary Gensler imploring the SEC to require companies to retain a cybersecurity expert on public boards, much like the financial expert required due to SOX.[16] Interestingly, it appears the SEC was listening and on March 9, 2022, proposed a ruling on this very topic.

SEC Proposed Rule on Cybersecurity Expert Disclosure

On March 9, 2022, the SEC proposed new rules for publicly traded companies to disclose material cybersecurity incidents in addition to cybersecurity risk management and governance. The proposed rules, which are available for comments, require that a material incident be disclosed in an 8k within 4 days of discovery by the company and disclosure of any previously undisclosed incidents which by themselves may not have been material, but in aggregate become material. In addition, the company must disclose policies and procedures for cybersecurity planning as well as disclosure of the board of directors' cybersecurity expertise. Although this new proposed ruling does not make it mandatory to have a cybersecurity expert on the board, it does offer a set of guidelines as to what being a "cybersecurity expert" means. In Item 106c of the proposal, the company would need to disclose whether the entire board is responsible for oversight of cybersecurity or if a specific committee is responsible. Also, the SEC is interested in the processes by which the board is informed about

[12] https://corpgov.law.harvard.edu/2020/09/15/boards-should-care-more-about-recent-caremark-claims-and-cybersecurity/
[13] Telephone interview with Mr. Luis Aguilar, former SEC Chairman from 2008-2015. Dated 10/21/2018 based on notes taken from the interview by me.
[14] S808, 117th Congress, First Session
[15] S808, 117th Congress, First Session
[16] https://www.reed.senate.gov/imo/media/doc/cybersecurity_disclosure_letter_to_sec_chair_gensler.pdf

cybersecurity risks and the frequency of discussions on the topic and whether and how the board or committee views cybersecurity risk as part of its risk management.[17] Finally, the SEC requests that the board identify any individual board members deemed to be cybersecurity experts. The SEC proposes a set of guidelines for what experience and education a cybersecurity expert should have:

- Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner.
- Whether the director has obtained a certification or degree in cybersecurity; and
- Whether the director has knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning.[18]

This is a non-exclusive list of requirements, however anything outside of these guidelines should be explained. The cybersecurity expert on the board will not be singled out for responsibility by the SEC, as the SEC indicated that cybersecurity planning and oversight is the responsibility of the full board. However, this new disclosure requirement does point to a potential in the future that the cybersecurity expert will become a requirement on boards much like a financial expert has due to SOX.

In a discussion with Luis Aguilar, former Chair of the SEC in October of 2021, he predicted that the SEC would create this disclosure requirement. Mr. Aguilar stated that although these individuals may be tasked with the oversight, the responsibility for cybersecurity compliance would fall on the entire board, not just the individuals. However, there will be more scrutiny of the individual experts and their actions during a crisis and the response by the board.[19] Mr. Aguilar's prediction has come true. The question is: will the SEC in the future take the next step to make a cybersecurity expert on boards mandatory?

The conclusion boards should draw from the heightened SEC disclosure requirements on cybersecurity is that the level of oversight that boards may have had in the past on cybersecurity is not enough at this time or in the future. As threats continue and escalate, the SEC and the Federal government will only get more constructive and intrusive into how a board and company manages cybersecurity risk. As noted earlier, asking questions isn't good enough, directors need to understand the answers. Interestingly, the threat cybersecurity creates to companies, the economy and the nation is very similar to the threat caused by the financial meltdown of Enron, WorldCom and Tyco in the early 2000s. At that time, the lack of accountability by the board and auditors involved with those companies allowed illegal and highly risky financial practices to run rampant. The result was close to an economic meltdown and the creation of Sarbanes-Oxley legislation and the ACFE. Looking at these parallels are helpful to consider what next steps may happen to lower cybersecurity risk across all industries.

Compelling Historic Parallels to Financial Expert – SOX and Enron

[17] https://www.sec.gov/rules/proposed/2022/33-11038.pdf
[18] https://www.sec.gov/rules/proposed/2022/33-11038.pdf
[19] Telephone interview with Mr. Luis Aguilar, former SEC Chairman from 2008-2015. Dated 10/21/2021 based on notes taken from the interview by me.

The logic for a potential requirement to have a cybersecurity expert on a board (as defined by either the company, SEC or NYSE or NASDAQ), sounds very much like the logic to have financial experts on the board and in the audit committee which focuses primarily on financial risk. The historical reason a financial expert is required on boards draws a strong parallel to the reason why a cybersecurity expert may be required on boards in the future. This parallel is best seen in the case of Enron. Enron and its financial meltdown are the genesis for much of what became Sarbanes-Oxley (SOX) legislation to provide more transparency in financials to investors. Although Enron's audit committee was reasonably financially astute, they did not question the validity of the information provided by either the company or the auditors. The massive amount of material covered in the audit committee made it difficult to opine or raise questions, and they lacked a level of independence due to many of their relationships with management and financial entanglements with the company.[20][21]

Due to the financial failure of Enron, WorldCom, and Tyco, which deeply affected the US economy in 2001 and the years to follow, Congress began legislation to provide more transparency and structure in public company reporting and board committee make up. Sarbanes-Oxley legislation created the rulemaking authority for the SEC in 2003 to require an Audit Committee Financial Expert (ACFE) adopted from SOX law section 407[22]. Attributes, education, and experiences are required for an individual to be considered an ACFE. The attributes are:

- An understanding of GAAP and financial statements.
- The ability to assess the general application of GAAP to accounting for estimates, accruals, and reserves.
- Experience preparing, auditing, analyzing, or evaluating financial statements of a breadth and level of accounting complexity generally comparable to that expected to be present in the company's financial statements (or experience actively supervising others engaged in such activities).
- An understanding of internal control over financial reporting; and
- An understanding of audit committee functions.

The experience required to be an ACFE are:

- Education and experience 1) in a position as a principal financial or accounting officer, controller, public accountant, or auditor, or 2) in a position involving similar functions.
- Experience in actively supervising a principal financial or accounting officer, controller, public accountant, or auditor (or an individual performing similar functions).
- Experience in overseeing or assessing companies or public accountants in the preparation, auditing, or evaluation of financial statements; or
- Other relevant experience.[23]

It is important to note that the SEC combines attributes, experience, and education to create a qualified ACFE. This combination is one that may be paralleled if S808 is passed, and a cybersecurity expert is

[20] The Fall of Enron; https://pubs.aeaweb.org/doi/pdfplus/10.1257/089533003765888403
[21] Audit Committee Memo Pillsbury Law;
https://www.pillsburylaw.com/images/content/1/4/v2/1402/59D80A391AF9E771B7A3BD899C2D5ED9.pdf
[22] https://www.cpajournal.com/2016/06/12/sec-audit-committee-financial-expert/
[23] https://www.cpajournal.com/2016/06/12/sec-audit-committee-financial-expert/

required. Also, NYSE and NASDAQ echo the requirement of a financial expert, and if an individual meets the requirements of the SEC, they also meet the requirements of NYSE and NASDAQ.[24]

SOX and the SEC created a massive change in how and what public companies report material information to the public markets. Some would argue that SOX and all the requirements it brought were too costly and onerous for many companies and as a result there are fewer publicly traded companies. But, when a company is public, the requirement to have a financial expert (or two or three) in the audit committee has brought about more critical examination of company financials, more accuracy in financial statements and better reporting on material company risk matters to investors. The benefits of transparency, oversight, and accuracy that a financial expert brings to a board, could be translated to a cybersecurity expert and their value on a board. Cybersecurity threats and technology are complex and fast moving. Understanding what technologies, processes, policies, and plans are in place, and whether they are enough takes technical, policy, legal, and governance knowledge. This kind of knowledge requires either experience or education. Much like a financial expert, those who have had responsibility for it or those who have had to personally oversee it can understand the implications of some of the choices companies make on cybersecurity. Leaving this to individuals who have business experience, but no technical, policy, or legal depth could mean exposure to risks and liabilities that the board doesn't understand. The SEC and the Federal government are moving toward understanding that knowledge and expertise in this area are critical – putting in place a requirement for an expert could happen in the next few years because of a cataclysmic cybersecurity event or concern that one may occur – both of which are highly likely.

What Companies are doing about it Now – Assessment of Fortune 20 Companies

To understand where boards are – or are not - in their journey toward putting a cybersecurity expert in the boardroom, a review of the proxy statements and 10Ks Fortune 20 largest public companies (based on revenue) is educational. Given that these are the highest earning and, in some cases, the most valued companies in the world, it would make sense that they have a high level of concern about cyber risk and may be leading the way in lowering risk in cybersecurity by having some cyber expertise on the board. After reviewing the 2021 proxies and 10Ks of the Fortune 20, the companies have a surprisingly uneven focus on cybersecurity. The following companies have been assessed (in alphabetical order):

1. Alphabet
2. Amazon
3. Amerisource Bergen
4. Apple
5. AT&T
6. Berkshire Hathaway
7. Cardinal Health
8. Chevron
9. Cigna
10. Costco
11. CVS
12. Exxon
13. Ford
14. GM

[24] https://www.cpajournal.com/2016/06/12/sec-audit-committee-financial-expert/

15. JP Morgan
16. McKesson
17. United Health
18. Verizon
19. Walgreens
20. Walmart

Several observations came from a review of each company's 2020 or 2021 10K and proxy statement.

1. 20 boards claim cybersecurity as a high risk for their company. Even though all the companies in the list name cybersecurity as one of the greatest risks for the company in their 10Ks, only 6 have cybersecurity expertise on the board, only 1 has a separate committee focused on cyber risk, and it is unclear how much time and attention is spent on cybersecurity policies, procedures, preparedness, frameworks, and infrastructure for the 19 boards that discuss cybersecurity in audit committee.

2. 19 boards noted above cover cybersecurity risk in audit committee. This means that with one exception all the boards do not believe cybersecurity risk requires a separate committee to focus on this area of risk. Given the massive digital assets each of these companies have and the level of threat implicit for them, it is hard to understand why they would not address cybersecurity risk in a separate risk committee. Of all public companies, these have the most to lose if attacked.
3. 18 boards have some technology expertise in audit committee. This is somewhat reassuring in that an individual in the audit committee has some context to understand and discuss cybersecurity issues. However, there are also problems with this in that audit committee covers a lot of material, most of which is financially oriented. A lot would depend on each board giving the committee enough time to thoroughly understand cyber issues during the meeting and have time to ask probing questions. It is very likely that given the amount of ground to cover in the audit committee meetings, cybersecurity is not given enough time and scrutiny. Also "technology" leaders may not have any background in cybersecurity. Although they may have some context for understanding security technologies, the likelihood that they could ask detailed questions about cybersecurity practices or preparedness is limited. Some of the technology the individuals have on the boards come from medical technology, or manufacturing technology. So, their ability to translate that into a meaningful dialogue on what a company is doing or not doing to prevent or prepare for or manage a cybersecurity attack is also very limited.
4. 1 board has a separate committee for risk and cybersecurity risk: General Motors. One other company has a risk committee, JP Morgan, however, that committee does not include cybersecurity risk. Walmart has a technology committee, but the technology committee does not address cybersecurity – and yet all the technology leaders on the board are in that committee.
5. 18 boards have some technology expertise on the board. This is reassuring that someone on the board has a level understanding of technology to make a broad assessment of cybersecurity risk and is conversant enough in technology to ask some basic questions. However, the kinds of technology backgrounds in the boardrooms vary and very few have any technology background in cybersecurity. Given the number of attacks that are occurring, and the sophistication of the attacks as well as the likelihood of nation state attacks occurring against many of these companies, just having an individual who has a technical background may not be enough to truly

understand the risk level, and probe deeply enough with the CISO and team to assure that the company is doing everything it can to lower risk.

6. There are 6 board members in the entirety of the Fortune 20 with self-reported cybersecurity specific knowledge. Given the changing technology landscape and kinds of attacks, specific, up to date knowledge of cybersecurity technology and practices as well as strong understanding of the current threat landscape is necessary to lower cyber risk. With only 6 individuals who claim cybersecurity expertise, and no information on what those claims entail, the Fortune 20 could be leaving themselves open to liability in the event of an attack.

Within the Fortune 20, GM stands out by creating a separate committee to oversee cybersecurity risk. The board has created a committee named "Risk and Cybersecurity Committee". It has the following charter:

Reviews the Company's key strategic, enterprise, and cybersecurity risks; Reviews privacy risk, including potential impact to the Company's employees, customers, and stakeholders; Reviews the Company's risk management framework and management's implementation of risk policies, procedures, and governance to assess their effectiveness; Reviews management's evaluation of strategic and operating risks, including risk concentrations, mitigating measures, and the types and levels of risk that are acceptable in the pursuit and protection of shareholder value; and; Reviews the Company's risk culture, including the integration of risk management into the Company's behaviors, decision-making, and processes.[25]

The committee is chaired by Linda Gooden, former Executive Vice President of Lockheed Martin's Information Systems & Global Solutions (IS&GS). Ms. Gooden has over 40 years' experience in technology and specifically IT. She oversaw a team of 40,000 IT professionals during her EVP role at Lockheed. It is exciting to see a leader of this caliber in IT chair a committee dedicated to cybersecurity risk. It also exceedingly rare and within the top 20 companies she is unique as is GM in this focus. An interesting question which I was unable to pose to the GM board, but that remains is why GM believes cyber risk is important enough to warrant both its own committee and chair that committee with a cybersecurity expert? One important note is that in reviewing the other members of the committee, none of the other committee members has any cybersecurity experience and only one other has experience as a technology leader.[26] GM's proxy statement discusses its focus on risk which considers "tops down and bottoms up" information enterprise wide. The CEO, Mary Barra is also the Chief Risk Officer and establishes the tone at the top for the company. There is also an established risk structure that runs from management to a Risk Advisory Council which advises executive level management who then advises the board. The Risk and Cybersecurity Committee is the committee on the board where enterprise-wide risk is discussed as well as cybersecurity risk.[27] This systemic approach to risk may be a best-in-class oversight practice, and one which should be considered by the other Fortune 20 and beyond companies. This focus on company level systemic risk may answer why GM has a Risk and Cybersecurity Committee. Operational risks in areas of manufacturing, supply chain, sales and product development are systemic – they are created and addressed across the company and can have a disastrous impact on a company's revenue and reputation. Cybersecurity risk is also a company level

[25] GM 2021 Proxy Statement
[26] GM 2021 Proxy Statement
[27] GM 2021 Proxy Statement

systemic risk - cybersecurity risks are created and addressed across the company and can have a disastrous impact on revenue and reputation.

In reviewing Walmart's audit committee charter as an example of audit committee specific duties, it is noted that Walmart's audit committee has 37 duties that it must manage over the course of 8 meetings a year.[28] Cybersecurity risk is noted in duty #8 which includes other types of risks as well. With 37 duties that the Walmart audit committee must attend to, cybersecurity risk may not get the attention warranted given the significance of the risk. Walmart has a separate technology committee with technology experts residing on the committee, however, Walmart chooses to address cybersecurity risk in audit committee which has 36 other duties to address and minimal technology expert representation. Walmart's audit committee charter is typical to audit committee charters across the Fortune 20. If that is the case, cybersecurity risk, given its complexity and the potential damage an attack can inflict on a company, is not given enough attention in audit committee.

As one reviews the information above on Fortune 20 questions come to mind. If Cybersecurity risk is claimed to be a top priority, why does only one company - GM – have a separate committee for overseeing cybersecurity risk? Why do only 6 of the companies have an individual who is a stated cybersecurity expert on their board? These are the largest companies in the world, so they are likely top targets for hackers and nation-state attacks. It would make sense given what these companies have at stake, the resources they have available to them, and scrutiny they are under from government, shareholders, and customers that they would ensure that at the board level they have enough time, attention, and expertise applied to cybersecurity risk. Overseeing cybersecurity in audit committee with a large financial agenda full of primarily financial experts, not cybersecurity experts, does not seem like enough.

The Case against SolarWinds Board – Proactive Oversight of Cybersecurity Necessary

On November 4, 2021, a case was filed against SolarWinds past and current board members and SolarWinds itself. The case alleges that under Caremark[29] the board breached its duty of loyalty and care for their "utter failure to implement or oversee any reasonable monitoring system concerning cybersecurity risks fundamental to SolarWinds' only line of business." The use of the foregoing sentence is very important as it establishes two parallels to a recent case before the Delaware court where the high bar of "business judgement rule" was cleared. The case which the SolarWinds case will likely parallel is the case against Bluebell Creameries Inc. – otherwise known as Marchand v. Barnhill.[30] In the case against Bluebell the two key issues on which the case turned were 1 - the fact that Bluebell was a monoline company, meaning it only has one product. 2 – the risk was a "mission critical" risk. Bluebell made ice cream. It was their primary product. In 2015 a listeria outbreak occurred due to Bluebell's ice cream that killed 3 and made many sick. Although Bluebell recalled their products, the company suffered a dramatic loss of revenue and eventually went bankrupt. According to Marchand lawsuit,

[28] https://stock.walmart.com/investors/corporate-governance/board-of-directors-committee-information/audit-committee/default.aspx
[29] https://corpgov.law.harvard.edu/2019/07/08/caremark-liability-for-regulatory-compliance-oversight/
[30] https://corpgov.law.harvard.edu/2019/07/08/caremark-liability-for-regulatory-compliance-oversight/

"Blue Bell's directors had failed to put in place a board-level oversight system for food safety—which was "mission critical" for the monoline company—and as a result had not received official notices of food safety concerns for several years."[31] In addition the court noted "that the complaint alleged that there was no board committee that addressed food safety; no regular process or protocols that required management to keep the board apprised of food safety compliance practices, risks or reports; and no schedule for the board to consider on a regular basis any key food safety risks that existed." Finally, the court stated, "*Caremark* does have a bottom-line requirement that is important: the board must make a good faith effort—*i.e.*, try—to put in place a reasonable board-level system of monitoring and reporting."[32]

The allegations against SolarWinds sound very much like Marchand. SolarWinds is a monoline company. SolarWinds has one platform, Orion which offers network management and monitoring. It has numerous features that can be enabled, but the company's one product is Orion. In addition, as a technology company which is deployed in over 300,000 networks globally cybersecurity is "mission critical" to the company – according to their 10K[33]. The SolarWinds board was warned by both the Defense Intelligence Agency and BugCrowd hacker, Vinoth Kumar that supply chain attacks were likely and that their password for updates was known publicly. [34] Also, the board, which is made up of primarily technology investors, reviewed cybersecurity in audit committee until the attack. Having no separate committee for cybersecurity risk, which is mission critical to a technology company again sounds much like Marchand which had established no separate committee and no known process to determine risk. Marchand establishes that in the case of a mission critical risk, duty of care and loyalty requires proactive and overt activities and processes to prove that a board is practicing oversight and is not negligent. In the case of Marchand as noted by Judge CJ Strine "On these facts," Strine held, "Although *Caremark* is a tough standard for the plaintiffs to meet, the plaintiff has met it here…in Blue Bell's case, food safety was essential and mission critical. The complaint pled facts supporting a fair inference that no board level system of monitoring or reporting on food safety existed."[35] Although the Caremark bar is possibly the highest in the legal world, judges have begun to infer that cybersecurity is a mission critical duty that boards must be proactive on. As Vice Chancellor Will said in the 2021 Marriott case, "cybersecurity risks are an increasingly important part of the corporate landscape, and as risks of cybersecurity become prevalent corporate governance must evolve to address them." She also added that "the corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place."[36]

If proactivity becomes a requirement to prove duty of care and loyalty, an argument can be made for the board to take two key actions.

---

[31] https://corpgov.law.harvard.edu/2020/05/25/recent-delaware-court-of-chancery-decision-sustains-another-caremark-claim-at-the-pleading-stage/

[32] https://corpgov.law.harvard.edu/2020/05/25/recent-delaware-court-of-chancery-decision-sustains-another-caremark-claim-at-the-pleading-stage/

[33] SolarWinds 10K 2021; https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/48bd02f7-3c52-4abc-a5e9-60401f9a4e8b.pdf

[34] https://www.moneytimes.com/articles/13892/20201216/SolarWinds-update-server-access-anyone-weak-password-security-expert.htm

[35] https://corpgov.law.harvard.edu/2020/09/15/boards-should-care-more-about-recent-caremark-claims-and-cybersecurity/

[36] https://www.dandodiary.com/2021/11/articles/shareholders-derivative-litigation/cybersecurity-related-breach-of-the-duty-of-oversight-claim-filed-against-SolarWinds-board/

1. Form a risk and cybersecurity committee in which mission critical risks – cybersecurity – can be overseen; and
2. Have an individual on the board who can understand at a detailed level the breadth of cybersecurity risks the company is facing and what the company can do to lower that risk.

This is exactly what SolarWinds has now done. The "technology and cybersecurity committee" is a separate committee and has at least one cybersecurity expert on it.

These recent Caremark cases may create more impetus for boards in the future to create a separate committee to focus on risk and cybersecurity. Even if the courts do not explicitly demand it, to lower liability and prove proactivity, boards should consider these changes in committees as well as board makeup to document the proactive nature of the board on cybersecurity risk.

Are Boards Demanding Cybersecurity Experts? Discussions with Board Recruiters

To understand the importance of cybersecurity expertise a discussion with board recruiters is helpful. Board recruiters are individuals in recruiting firms that specifically focus on board opportunities. Three board recruiters from the leading recruiting firms, Heidrick and Struggles, Korn Ferry, and Russell Reynolds were interviewed to understand if boards are looking for cybersecurity expertise, and if not why and what is their strategy to apply some level of cybersecurity knowledge on their board. The answers were consistent. Boards are not looking for cybersecurity expertise on its own. Boards equate cybersecurity expertise with a CISO, and they all believe that a CISO is too narrow to be able to understand broader strategic considerations in a boardroom. CISOs are functional experts, with limited business background, and cannot offer opinions on broader corporate issues. More often companies are interested in putting a technology leader or a digital technology leader on their board. Someone who has transformed a large company or a business leader with strong technology background. Broad knowledge across numerous areas of business is required and functional expertise isn't as valued. Boards are more focused on diversity and culture as ESG requirements for boards have grown. Diversity on boards is seen as a more pressing issue than cybersecurity.

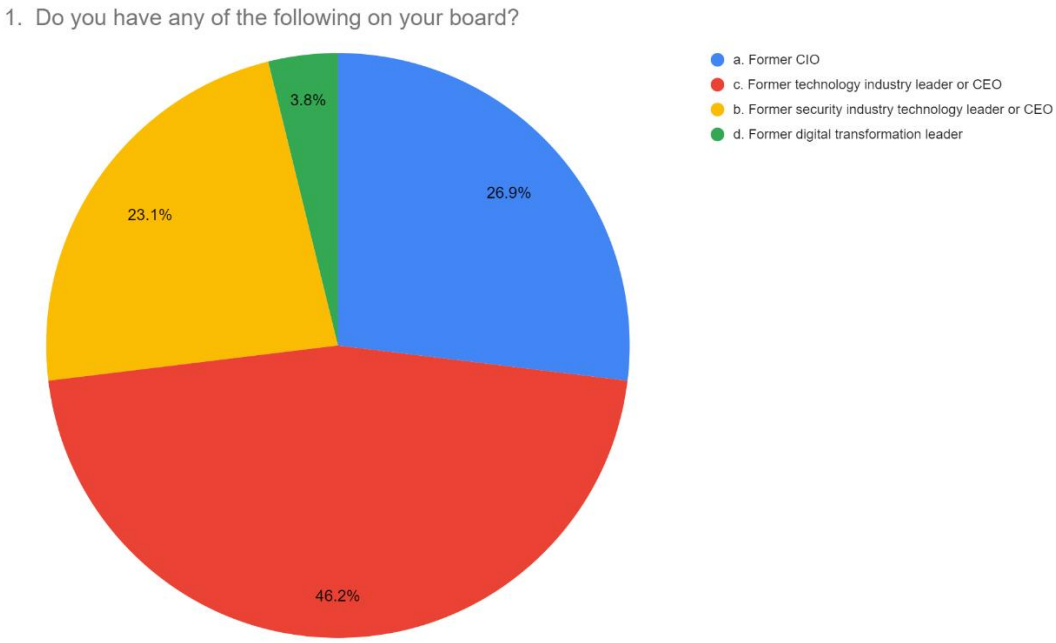
The recruiters indicated that boards believe they can utilize the CISO in the company to train board members to understand cybersecurity and the attendant risks. This seems like an incomplete choice given that the CISO may or may not be giving the board the full picture of the cybersecurity risks of the company or may not be able to help the board understand the technical details of cybersecurity. In addition, most boards believe that if they have a technology leader on their board, that is sufficient to understand and lower cybersecurity risk.[37] However, given the complexity of cybersecurity as a technology, and the fast-moving nature of threats, just having a technology background may not be enough to prepare for and handle a cybersecurity attack. As seen in the SolarWinds attack, the board members were reasonably technical, and yet, they did not prevent one of the worst systemic attacks in the history of the US. They didn't even know an attack had occurred until months later when another company, FireEye informed them that a breach had occurred, and they were injecting malware into their customers networks via an update.[38]

[37] Interviews with Selena LaCroix, Lee Hansen, Charles Tribbett, 7/2021

[38] https://www.csoonline.com/article/3613571/the-SolarWinds-hack-timeline-who-knew-what-and-when.html

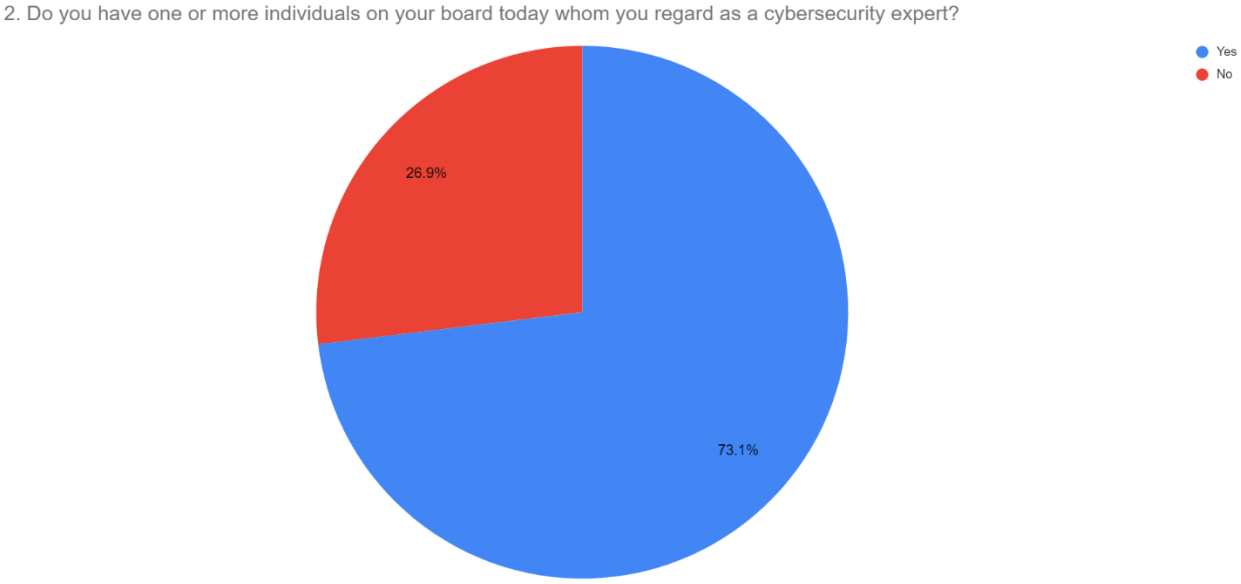
Board Member Opinions on Cybersecurity Expert – Are they For or Against?

To understand the importance of a cybersecurity expert on boards today, as well as board members thoughts on the level of concern about cybersecurity, a survey was conducted in December of 2021 and January of 2022 of 240 board members from public company boards. 200 of the board members belong to Women Corporate Directors organization chapters in Northern and Southern California as well as Hawaii. The additional 40 board members belong to smaller networks and those who serve on boards with me. All surveyed responded based on one of their boards - not a response for each board they serve on. 26 individual responses were received, which is a ~10% response rate – an average response rate for an external survey.[39] The following results were gathered from the survey.

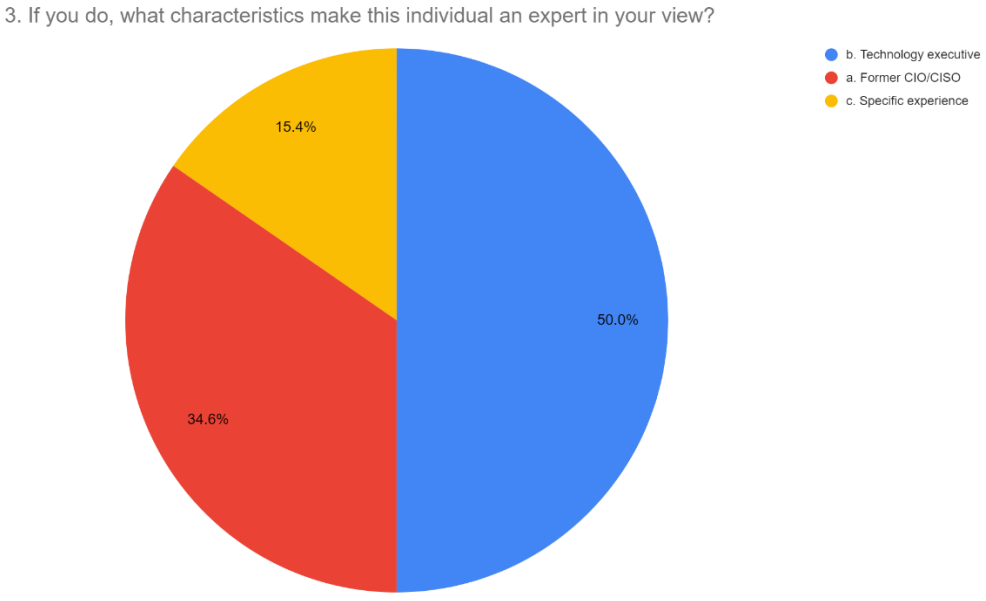


It is interesting to note that the majority of directors surveyed have technology leaders on their board. A disappointing 23.1% have a security industry expert on their board.

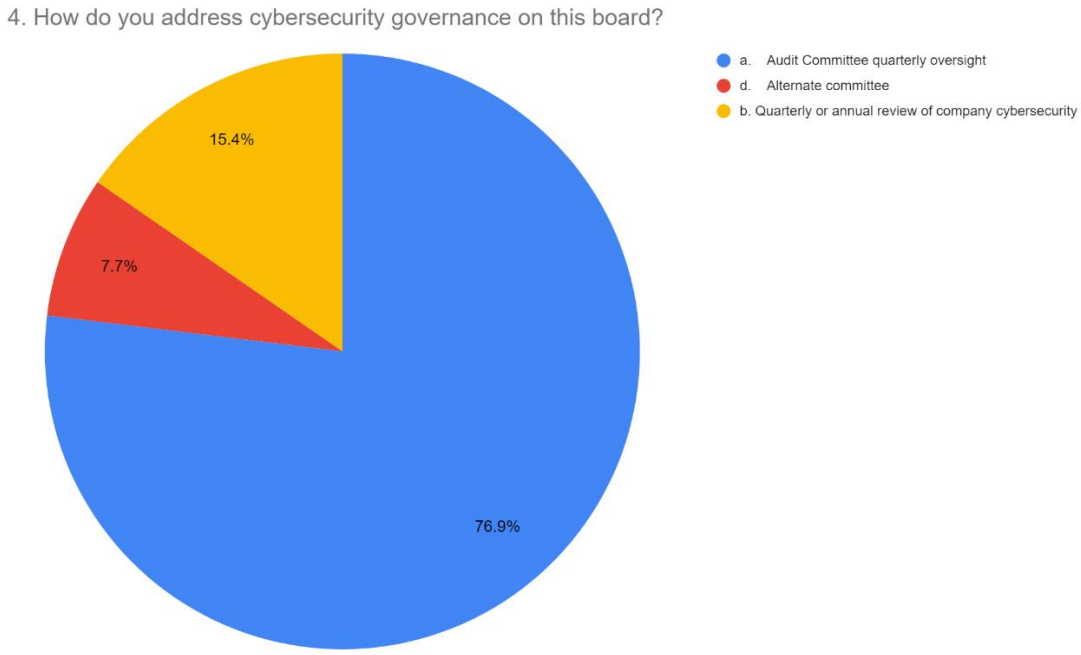
[39] https://www.smartsurvey.co.uk/blog/what-is-a-good-survey-response-rate



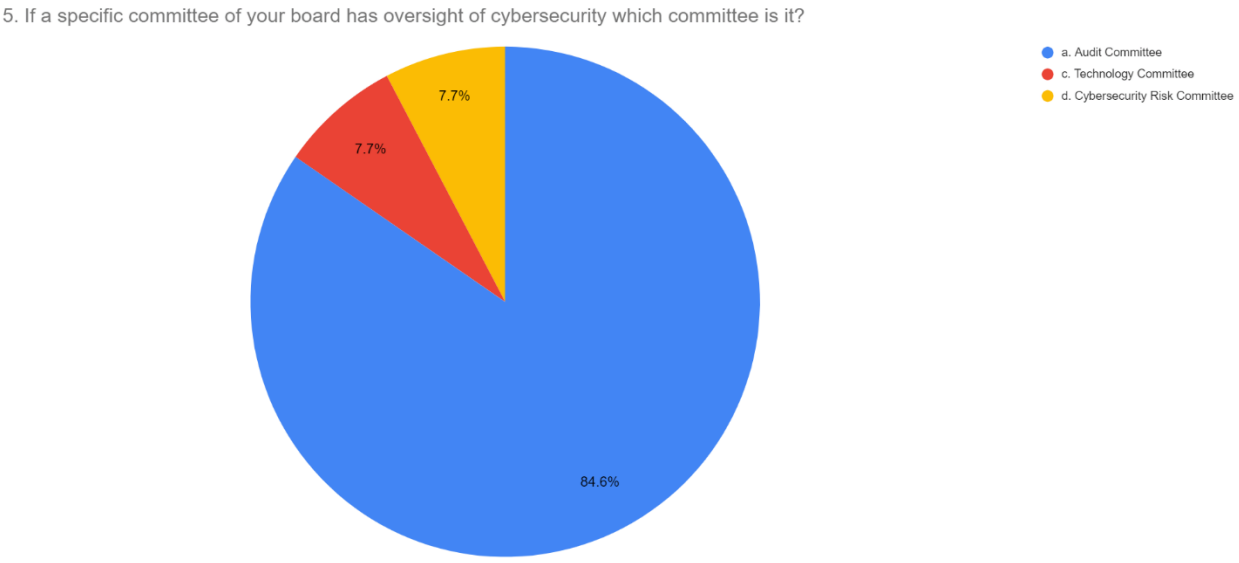
This question highlights the belief among board members that technology leaders have cybersecurity expertise. Unfortunately, this is not often the case as technology knowledge does not often cover cybersecurity. Many of the technology leaders on these boards are focused in very different areas of technology such as biotechnology, and digital transformation.



50% of those considered “experts” are due to technology leadership. This is not equivalent to cybersecurity expertise.

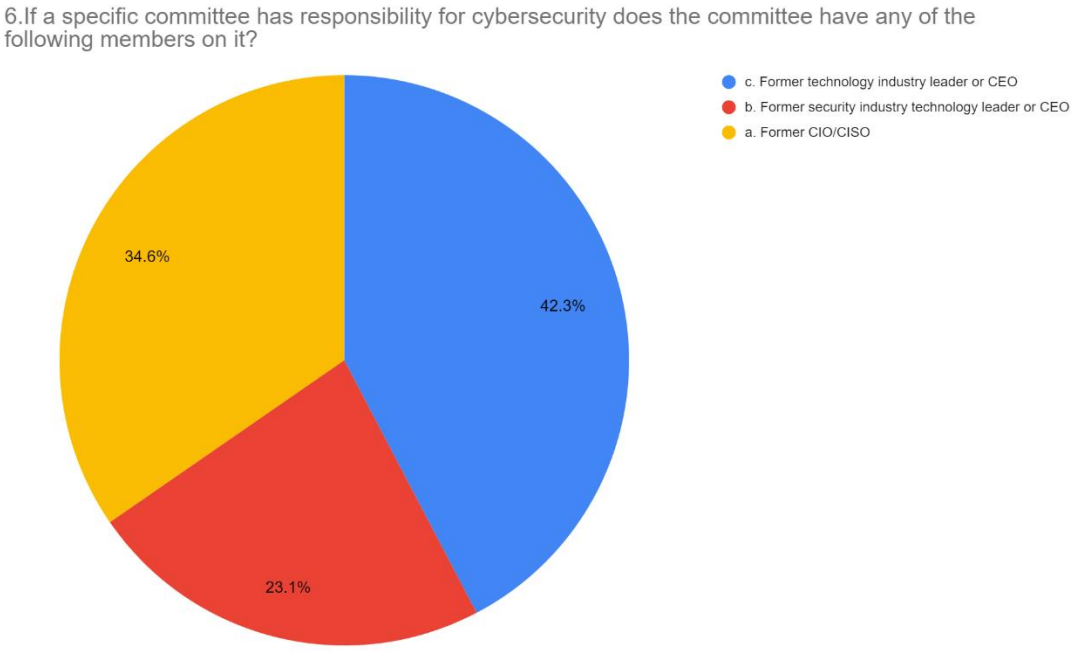


76.9% of board members surveyed indicate that they address cybersecurity risk in the audit committee. While only 19% of board members surveyed utilize an alternate committee.

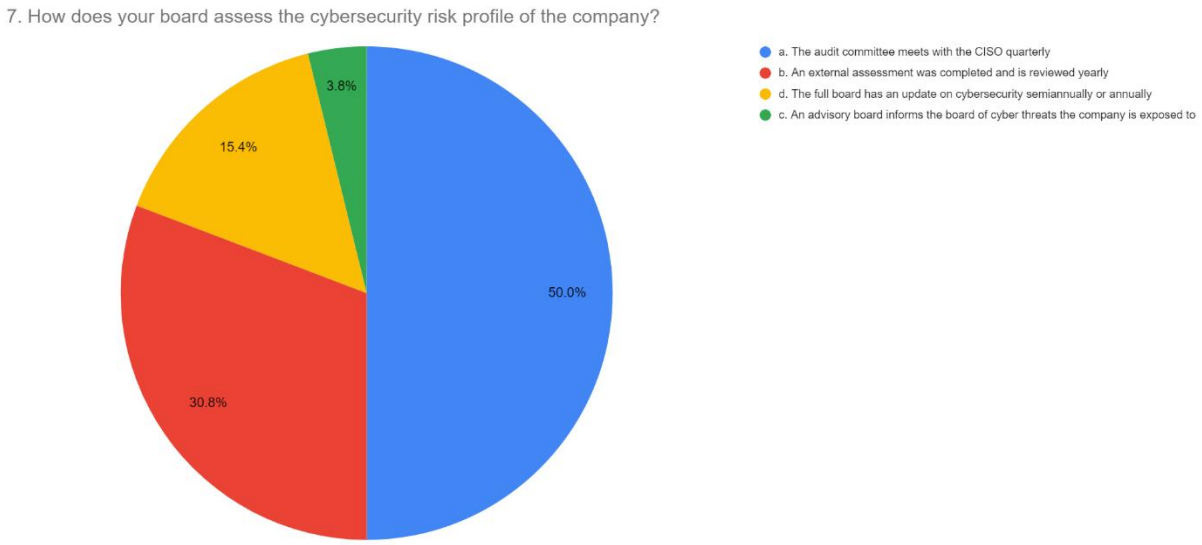


There are a small percentage of board members surveyed who indicate their board utilizes a cybersecurity risk committee. However, 84.6% utilize audit committee to address cybersecurity risk as noted in the prior question. As noted previously, the audit committee has numerous agenda items and

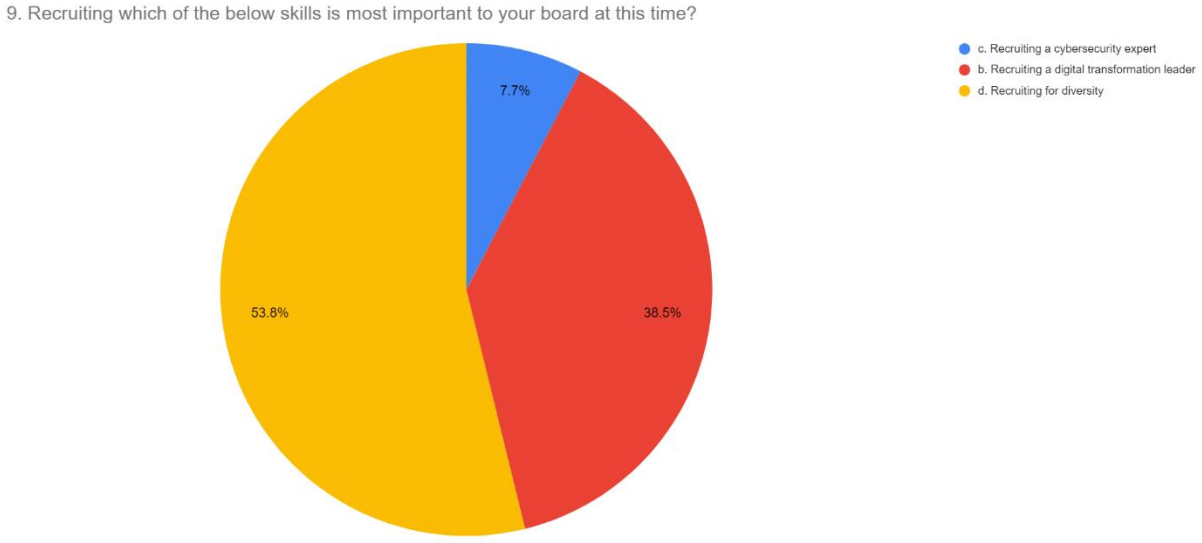
most individuals in the audit committee are financial experts, not cybersecurity experts. There are also a small number of board members who indicate their board utilizes a technology committee to address cybersecurity, this is a positive step as the committee will likely contain technology leaders and the focus will be on technology and cybersecurity as part of technology.



The good news is that close to 70% of the committees that have cybersecurity responsibility have a technology leader in the committee. The issue with audit committee extends beyond the skillset in the committee to how much time and focus is given to cybersecurity within the committee. The agenda is very broad ranging and packed with financial topics. It is unclear how much time and attention cybersecurity are given. In addition, it is not known how many meaningful dialogues and questions are being asked.



Half of board members surveyed are reviewing cybersecurity quarterly in the audit committee with the CISO. Also, 30% have an external assessment of cybersecurity yearly. This provides a strong baseline for understanding the company's risk profile and how well the company is progressing in its cybersecurity goals. However, the question of how impactful the discussions on cybersecurity in audit committee remains. Are the questions probing enough? Is there enough time allotted to discuss it? If there is one technology leader in audit committee, are they the only one who understands what the CISO is talking about?



According to the survey currently 7.7% of board members indicate their board is recruiting a cybersecurity expert. This is quite low as compared to recruitment for diversity and digital transformation. Digital transformation is viewed by board members and recruiters as a broader skill set

that encompasses business knowledge as well as technical savvy. It is also considered a positive game changer for many companies at this time.

Many comments were received from board members that elucidate their opinions about cybersecurity expertise on boards. When asked "What are your thoughts about having a cybersecurity expert on the board? Please explain." Board members overall indicated that it is important but are concerned with the narrowness of experience. There is interest in having board members learn more about cybersecurity, but most boards rely on the strength of the company's CISO and CIO to provide expertise. One board member commented: "I think boards need more cyber security expertise on the board and the committee that oversees the risk. I also believe that the other members of the board/committee need to get reasonably cyber literate; it can't be all on the shoulders of 1 or even 2 board members." Another indicated: "Important (if not essential). Helps to drive the cybersecurity policies for the company; ensures the board has comprehensive and timely discussion regarding risk and appropriate policies; prioritizes discussion; resource for company leadership team."[40]

Some companies utilize external advisors and assessments as well as industry benchmarks to understand how well they are doing against their peers and where they should be investing.

When asked: "If there were a requirement for a cybersecurity expert what attributes or experience do you think would be important?" Respondents answered that a former CIO or CISO is valuable, but they must have a broad business background as well.

One respondent commented: "Executive experience as a CISO or CSO; or executive experience at a cyber security company. Understands enough of the details so that the person can help provide effective oversight and governance. Knows the most important questions to ask and be able to assess validity/effectiveness of management's approach/responses. Stays current with evolving cybersecurity landscape. Takes the time to understand the business well, so that cybersecurity strategy is most appropriate for the particular organization and its business."

Education of the board was of interest, but the individual expert did not necessarily need education to be deemed an expert. Broadness in both experience and thought were the key for a candidate – "Also they must understand your company's industry and be a broad level thinker. They need to add value in places like strategic and organizational discussions, not just cyber risk."

After assessing the results of the survey, several conclusions can be drawn:

1. Cybersecurity is important to board members, and they spend time in the board room understanding the risks and the status of their cybersecurity programs and processes.
2. Audit committee is the primary committee that addresses cybersecurity risk. The good news in the surveyed companies is that most of them have a technology leader

[40] Cybersecurity survey

in the audit committee who may possibly understand cybersecurity. Although many acknowledge that the technology leader is not a cybersecurity expert.

3. Cybersecurity expertise is valuable. Individuals who understand cybersecurity and the risks and liability for the company and the board are of interest to boards.
4. Those who have cybersecurity knowledge must stay current to be of value and they must have a broader perspective on business issues and strategy for the company.
5. Education is not necessary – experience and skills are valued.
6. Although board members find cybersecurity expertise valuable, their top priority for recruiting is diversity.

As noted in the survey, 80% of board members indicated that their board addresses cybersecurity risk in audit committee. Also, it was noted that 70% of board members indicate that their board has one technology leader in audit committee. The next question one might ask is what are the specific duties of the audit committee? Even if the audit committee reviews cybersecurity risk as part of the agenda, and the committee has a technology leader who can possibly understand cybersecurity issues, how much time and focus are allotted to cybersecurity on a quarterly basis?

A typical audit committee charter as noted by Deloitte has 40 duties that it is responsible for. These duties are massive and range from financials and financial disclosures to internal and external audit, internal control structure, ethics and compliance, financial and cyber risk, reporting, accounting policies, and accounting information review.[41]

EY noted that 68% of Fortune 100 boards address cybersecurity risk in audit committee[42], which may or may not have technology or cybersecurity expertise. Does this mean that companies and boards are potentially more exposed to cybersecurity risk? Are boards doing enough to assure that they can ask the right questions, understand threats, limit liability, and lower risk for their companies. Given the sophistication and potential damage of the threats, the escalated focus from the SEC and federal government, the new liabilities that are emerging in case law, and the constantly changing technology landscape, boards today may not be doing enough to lower risk in this area and more cybersecurity expertise on boards is needed. The most direct approach is to hire a cybersecurity expert on the board. However, the profile of that cybersecurity expert can vary, and a combination of skills, experience, and education must be considered.

What Would the Profile of a Cybersecurity Expert Be?

The profile of a cybersecurity expert doesn't necessarily mean that the only candidate for the job is a former CISO. The worry about a former CISO being too narrowly focused may be overemphasized, as

[41]https://www2.deloitte.com/content/dam/Deloitte/il/Documents/risk/CCG/sample_audit_committee_charter.pdf

[42] https://www.ey.com/en_us/board-matters/cybersecurity-risk-disclosures-and-oversight

many CISOs are strong business leaders as well as technically capable. However, a job title should not be the deciding factor when boards consider who a cybersecurity expert could be.

Reflecting on the SEC cybersecurity expert disclosure requirements and the parallel of a financial expert, an ACFE a combination of attributes, experience and education should make up the requirements.

Attributes:

- Understanding of basic information technology.
- Understanding of cybersecurity risk and governance.
- Understanding of basic cybersecurity technologies.
- Understanding of the regulatory requirements and measurements of cybersecurity oversight.

Why are these attributes important? The attributes enable an individual to have context to understand the cybersecurity plans, risks, and preparedness of the company. Information technology is the broader context in which cybersecurity resides, so understanding that context is important to then understanding how the cybersecurity technologies are used and why they are necessary. The basics of cybersecurity technologies is also important, again for context. Knowledge of regulatory requirements to understand how well a company is complying and frameworks such as NIST and CSM would enable the board to measure the company's preparedness to aid in preventing an attack and preparedness in the event of an attack. To ask intelligent and probing questions, and understand the answers one receives, these attributes are critical.

To qualify the individual must have gained the foregoing knowledge through **one** of the below:

- Experience as a CISO or CIO deploying or overseeing deployment of cybersecurity technologies.
- Experience as a CEO, CTO or CPO, Head of Engineering in a company which sells, or deploys cybersecurity products or infrastructure.
- Experience as a consultant or investor whose practice focuses on cybersecurity.
- Education or training through a certification program or degree level program in cybersecurity.
- Knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning.

Experience either in the field of cybersecurity or as a technology leader with training in cybersecurity will provide hands on knowledge of circumstances and challenges in cybersecurity. Experience overseeing security planning at an operational level or gaining certification or degree or using one's technology experience provides the ability to know when a threat is imminent or how serious it may be or what additional steps the company must take to lower risk. Actual experience or training is critical given the complexity of cybersecurity technologies and constantly changing threats. Knowledge or skills in security policy and governance, risk management, business continuity planning, incident handling, security operations and control evaluation all enable an individual to understand how to analyze risk or what to do when an incident occurs.

In addition, it is important for the cybersecurity expert to stay up to date in attacks, threats and new techniques and tools. Because the cybersecurity landscape is changing constantly, ongoing training is necessary for the cybersecurity expert as well as the entire board.

Conclusion

Over the last five years, US companies have seen a massive increase in the amount, variety, and sophistication of attacks. The loss of personal and confidential information, billions of dollars in stock value, IP, and financial loss, and damage to companies and individuals will only continue to increase in the future. As we have seen the SEC and the federal government are requiring more disclosures on cybersecurity disclosures and enforcing penalties on companies and their boards even when there has not been a breach.[43] There are cases pending in Delaware Chancery Court that make it clear that proactive, documented board governance and oversight combined with a committee focused on cybersecurity will reduce board liability. Finally, there is the new SEC proposed ruling that will require disclosure of cybersecurity incidents and cybersecurity expertise on boards. Given the SEC history of a financial expert requirement on boards, it seems likely that the next step would be an SEC requirement for at least one cybersecurity expert on public boards.[44] If that is the case, the time to put a cybersecurity expert on boards is now before boards must scramble to do so.

With all that is at stake most boards have not moved cybersecurity risk out of audit committee which is overburdened with financial risk, and they have not made hiring a cybersecurity expert to the board a high priority. Even though it is hard to understand why change has not occurred at this time, change is needed. Cybersecurity is a complex and constantly changing risk that deserves time and attention from a board beyond the audit committee and deserves the focus of an individual with a cybersecurity skill set who deeply understands all aspects of the cyber threat potential. Two key changes should be made on boards immediately:

1. Create a separate risk committee or technology and cybersecurity committee. This would provide the time and attention the subject deserves.
2. Add a Cybersecurity expert to the board. This would lower risk dramatically and provide value beyond cybersecurity.

These two actions would have a huge positive impact on lowering company level security risks across industries while lowering the level of systemic risk in the US economy.

[43] Harvard Law School Forum on Corporate Governance; SEC returns spotlight to Cybersecurity Disclosure Enforcement; 8/1/2021

[44] https://www.forbes.com/sites/bobzukis/2022/04/18/the-sec-is-about-to-force-cisos-into-americas-boardrooms/?sh=2a1f2d8168a9