CISA
CYBERSECURITY
ADVISORY
COMMITTEE

REPORT TO THE CISA DIRECTOR

Corporate Cyber Responsibility

September 13, 2023

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established the Corporate Cyber Responsibility (CCR) subcommittee to research ways to encourage a nationwide culture of corporate responsibility where cyber safety is incorporated into all executive decisions and how to encourage, enable and support private sector boards and C-Suite executives to reduce cyber risk as a matter of good governance. Cyberattacks and their impact could be better mitigated or even prevented if corporate boards of directors were more educated and engaged on matters relating to cybersecurity, placed a higher priority on cyber resilience, and exercised stronger oversight over the development and execution of their companies' cybersecurity strategies.

CISA provided an initial set of six framing questions to guide the work. These questions are below, with corresponding notations as to where each question is addressed within this report:

1. How should CISA work with board members and shareholders of public companies to encourage them to take a more active role in cybersecurity?
   This question is addressed throughout the report within multiple recommendations.

2. How can CISA help board members and shareholders understand the impacts of companies' cyber risk management practices and advocate for the adoption of cybersecurity best practices?
   This question is addressed throughout the report within multiple recommendations.

3. How can CISA best structure its guidance and outreach so it reaches board and C-Suite audiences? How should this outreach differ, if at all, for public and non-public companies?
   This question is addressed throughout the report within multiple recommendations.

4. How can CISA measure the effectiveness of the CCR effort?
   See recommendation within Pillar IV/Sustained Leadership and Collaboration concerning the designation of a high-level CISA official with industry experience who should have responsibility for overseeing and measuring the effectiveness of CISA's CCR effort.

5. What lessons can CISA draw from movements that have sought to use shareholder or board influence to change company practices, for example, on environmental or social issues?
   See recommendation within Pillar I/Board Member Education intended to bring cyber resilience to the forefront of investor decision-making.

6. Should CISA encourage credit rating companies to establish ratings of companies' cyber risk? If so, what should they measure? What are the possible downsides of introducing such rating systems?
   See recommendation within Pillar II/Measurement concerning the use of tools developed by credit ratings companies that may assess cyber resilience, readiness, or compliance.

The recommendations were informed by a series of briefings involving participants from corporate governance and corporate cybersecurity governance communities. It divided its work into three main phases:

1. Evaluating the lines of effort (LOEs) that CISA currently has to draw more attention to the specific actionable steps board members and C-Suite corporate officials can take to better secure their companies (including working with national organizations representing these stakeholders);
2. Exploring drivers and potential drivers of director behavior to understand how best to motivate them to take a more active role on cybersecurity matters; and
3. Developing actionable recommendations to CISA for how to encourage the behavior it seeks from corporate boards relating to how to ensure directors and management understand that cyber risk is one of several business and operational risks and that managing it is critical to a company's financial health.

Findings

High-profile breaches, especially those that have occurred over the past few years, have impacted a wide array of public corporations, and drawn national attention to the risk that cyberattacks pose, not just to business continuity and profitability but to the continuity of our society. Ransomware is having devastating effects on U.S.-based companies and organizations and the citizens that rely on services provided by them, especially those in critical sectors. The current cyber threat against American corporations and by extension the U.S. economy is of the same level of magnitude and seriousness as the conditions that led to the 2001 world financial crisis. Corporate financial scandals involving Enron, WorldCom, and other companies ushered in a new era of accountability for public company directors. The impact of the crisis was so profound that the government, among its many responses, created more robust standards for corporate oversight and accountability. These standards included new rules concerning board independence, the implementation and strengthening of internal control systems, and restrictions on the provision of non-audit services by external auditors, just to name a few. Over the past three years, U.S. corporations have faced cyberattacks that pose an extreme level of risk. It is estimated that by the year 2025, cybercrime will cost the world $10.5 trillion annually.[1] IBM has estimated that the average cost of a data breach globally is $4.45 million.[2] Recent notorious attacks have included the SolarWinds, Colonial Pipeline, Log4j and, more recently, the MOVEit breaches, as well as the insidious ransomware epidemic that seems to disproportionately affect vulnerable critical sectors (e.g. education and healthcare) and small businesses. This dire trend necessitates that the U.S. government and CISA take serious action to stem the crisis and curb future risks from threatening the continuity of our sectors, economy, and society. Increased corporate responsibility must lie at the center of these actions, much as it did in the wake of the world financial crisis.

The members of the Subcommittee have significant combined experience serving on, communicating with, and supporting corporate boards. Individuals in this group have struggled with or witnessed first-hand the barriers to effective board governance of cybersecurity and are pleased to offer their recommendations to the CISA Director. The recommendations generally can be categorized into four main areas (Pillars): **Board Member Education, Measurement, Responsibility and Sustained Leadership, and Collaboration.**

I. **Board Member Education**: The U.S. must find a way to eliminate the "cyber literacy chasm." There is a major gap in the knowledge directors have of cybersecurity issues broadly and about the components of strong cybersecurity programs. There will never be enough Chief Information Security Officers (CISOs) to staff every board, and it is imperative that board members develop more cyber literacy and competency. Not every board member needs to be an expert in understanding and addressing the cybersecurity concerns of the company, but more board members need to be far better educated on how to understand cyber risk, how to better listen to and understand CISOs, and how to better evaluate the effectiveness of their companies' cybersecurity plans. All board members should have a basic level of education on cybersecurity issues. Education also means CISOs should be enabled to become more effective listeners and communicators with, and to, directors. More education on both sides will enable a more effective and sustained relationship between directors and CISOs. Efforts to educate board members about cybersecurity are not new: leading stakeholders including the National Association of Corporate Directors (NACD), Diligent Corporation, the Institute for Shareholder Services (ISS), and NASDAQ have created some highly effective approaches. Efforts to make CISOs more adept at communicating

[1] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[2] https://www.csoonline.com/article/567697/what-is-the-cost-of-a-data-breach-3.html

with boards are also not new, and here we point to the work of Digital Directors Network (DDN), ISC2 and others. While very effective, these efforts have not necessarily been able to scale to the extent that is needed to account for the multitude of U.S. corporate boards in need of this transformation.

II. **Measurement**: There needs to be improved data and metrics concerning the level of cyber literacy and competency of directors. Additionally, there must be more availability and uniformity of data concerning cyber risk within enterprises to enable both CISOs and directors to perform their duties. Directors must have access to relevant and timely information, avoiding excessive filtering through management layers, and be able to use that information to assess cyber risk and performance and, with firm management, implement changes.

III. **Responsibility**: There must be clearer lines of responsibility and accountability drawn between stakeholders responsible for ensuring the cyber resilience of corporations. This conversation has been accelerated by the Securities and Exchange Commission's (SEC) proposed cybersecurity rules that would require publicly traded companies to disclose a cyber incident within four business days upon determination of materiality and to provide disclosure in periodic reports about certain cybersecurity governance practices. While CISA does not have jurisdiction over requirements for corporate boards, it can play an important role in shaping the conversation about what is expected of companies and their directors. This Pillar will discuss how to encourage board members to take a more active role in cybersecurity, will recommend the creation of best practices for board governance and then suggest ways to ensure corporations are following these best practices. This Pillar will also suggest ways to ensure boards and corporations follow cybersecurity best practices including through new or amended requirements relating to the implementation of known cybersecurity risk management frameworks and the creation of principles and accompanying best practices for cyber-responsible boards. It will also discuss the question of board structure.

IV. **Sustained Leadership and Collaboration**: Directors are becoming more involved in matters of cybersecurity governance as the risks and impacts associated with cyberattacks have an outsized impact on company performance, reputation, and liability. While cybersecurity issues are much more broadly discussed and understood today, CISA, in partnerships with other stakeholders, can do more to incentivize directors to be more engaged and give them the tools exercise more diligent and informed oversight. CISA has been providing crucial leadership on corporate cybersecurity governance by creating various guidance documents and collaborating with stakeholders to address specific needs. CISA released the Cybersecurity Performance Goals (CPGs), which establish a common set of fundamental cybersecurity practices for critical infrastructure with known risk-reduction value.[3] CISA continues to work with both Sector Risk Management Agencies (SRMAs) and industry to develop Cross-Sector Cybersecurity Performance Goals that will address safety practices that may be unique to a given sector, as well as sector-specific approaches to implementing the cross-sector goals.[4] CISA also worked with the NACD in the development of an updated Director's Handbook on Cyber-Risk Oversight and to create the Certificate in Cyber-Risk Oversight Program[5] for mature boards ready to take an additional step in cybersecurity oversight. This Pillar will recommend ways CISA can strengthen the cooperation amongst all stakeholders in this ecosystem and leverage and build upon work that is already underway. Implementing the recommendations in this report will require CISA to dedicate more personnel to corporate cyber responsibility, including a designated senior staff leader with several direct reports, to coordinate and oversee CISA's ongoing CCR efforts and to ensure it has sustained and structured partnerships that allow it to team with the right stakeholders to accomplish these objectives.

With respect to time horizon, several of the Subcommittee's recommendations warrant immediate attention. The Subcommittee designates such recommendations by stating that they should be implemented "as soon as practicable." Five of the recommendations included in this report fall into this category: Obtaining the necessary data about the gap in director education about cybersecurity (Pillar I/Board Member Education/1); Expanding and enhancing educational

[3] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
[4] https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf
[5] https://www.nacdonline.org/events/detail.cfm?ItemNumber=37092

offerings and training for directors (Pillar I/ Board Member Education/4); Obtaining the necessary data to assess how well directors provide oversight to firms on cybersecurity matters (Pillar II/Measurement/1); Developing Performance Goals for Cyber-Responsible Boards that advances a set of principles and best practices for cyber-responsible boards (Pillar III/Responsibility/5); and Designating a high-level official to lead a line of effort around increasing national corporate cyber responsibility (Pillar IV/Sustained Leadership and Collaboration/1).

The Subcommittee agreed that it was crucial to first identify the potential and actual drivers of director behavior to inform its recommendations. These drivers are key to motivating directors to become better educated, engaged, and accountable on matters of cybersecurity. After considerable discussion internally and with subject matter experts, the Subcommittee summarizes these drivers as follows:

1. **Regulations:** That directors' behavior is directly and strongly influenced by regulations, both federal and state, needs little explanation. Regulations can pertain to high-level governance issues, or they can contain mandates to implement specific security controls. An example of the former includes the SEC's proposed Cybersecurity Risk Governance Rule for Public Companies, which contains mandates around governance issues such as required disclosure of cybersecurity policies and procedures and providing adequate information to shareholders.[6] Examples of the latter include the Transportation Security Administration's (TSA's) Security Directive for Pipelines or the New York Department of Financial Services' 23 New York Codes Rules and Regulations (NYCRR) Part 500.[7,8]

2. **Audits:** Auditors conduct assessments of how well companies have met the aforementioned regulations. These assessments generate findings, which in turn require management, with the approval of directors, to take specific corrective actions. The requirement that a company reports material weaknesses or significant deficiencies relating to cybersecurity will, over time, alter director behavior more than any other single driver, as evidenced by the effectiveness of controls required of companies by the Sarbanes-Oxley Act of 2002. This is addressed in Pillar II/Measurement (Measuring enterprise cyber risk) and Pillar III/Responsibility (Create common controls, measurement, and reporting).

3. **Civil and criminal liability**: Class action lawsuits send a strong signal to directors and management that there exists a duty of care to stakeholders that must be followed. The case of one Uber executive being found criminally liable for not disclosing a breach of consumer data serves as a powerful example.[9]

4. **Risk transfer markets:** The availability and cost to companies of insurance policies that cover the effects of financial risk resulting from cyberattacks impact board behavior. In underwriting cybersecurity insurance policies, insurance companies have an extensive list of questions companies must answer. If companies do not maintain strong cybersecurity programs, including following known frameworks, then insurance policies will be much more expensive or even unavailable.

5. **Brand risk**: When a breach or cyber incident becomes public, companies can suffer a degradation of their brand, which in turn diminishes shareholder value. Board members will therefore endeavor to reduce brand risk owing to cyberattack by diligently overseeing cybersecurity programs.

6. **Duty of care:** Cybersecurity regulations commonly directed by specific U.S. federal agencies at companies within critical sectors under their purview are usually derived from National Institute of Standards and Technology (NIST) Special Publication 800-53. Yet not all publicly traded companies are considered to fall within "critical

[6] https://www.sec.gov/news/press-release/2023-52-
[7] https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf; https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
[8] https://www.dfs.ny.gov/industry_guidance/cybersecurity
[9] https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-sentenced-three-years-probation-covering-data

sectors" and are therefore not required to implement a specific set of controls such as these frameworks prescribe. Many companies adopt NIST 800-53 or the NIST Cybersecurity Framework (CSF), or another cybersecurity risk framework such as the Center for Internet Security (CIS) Controls, MITRE ATT&CK framework, or the CPGs. But for many companies, following such a cybersecurity risk management framework is not required. Companies should, however, adopt one of these frameworks because they are increasingly providing the elements for the duty of care (i.e. minimum expected actions) for corporations to ensure cyber resilience. Especially when combined with some of the aforementioned drivers (e.g. civil liability), these frameworks as well as any additional future cybersecurity requirements placed upon companies have a powerful influence on director behavior.

7. **Investor Awareness:** Directors have become increasingly more educated and aware of environmental, social, and governance (ESG) issues because institutional investors and pension funds are considering the environmental and social impact of their portfolios to a far greater to degree. We must strive to ensure investors are educated about the impact of cybersecurity risk within their portfolios.

Recommendations

Pillar I/Board Member Education

This Pillar addresses the most critical education gap, which is the need to create stronger cybersecurity knowledge and expertise among board members.

- Produce a report on the board director education gap. As soon as practicable, CISA should initiate a collaboration with relevant stakeholders to produce a data-driven report that enumerates the cyber literacy gap in the boardroom.
  - Relevant and accurate data is needed on the cybersecurity literacy of directors on U.S. corporate boards to understand the scope and impact of the problem as well as to define the knowledge gap that exists between board members and CISOs. CISA should conduct an assessment on the "state of cyber literacy in the boardroom" that measures and describes the cyber literacy gap that exists between directors and CISOs. A section of this report should be devoted to assessing the literacy gap of directors of non-public companies.
- Establish expected levels of cybersecurity knowledge for board directors. CISA, in coordination with other stakeholders, should create and promote an expectation of the baseline level of knowledge about cybersecurity all directors should have and should create recommendations for a standardized cybersecurity curriculum for directors to be incorporated into training offerings.
- CISA, in coordination with other stakeholders, should determine levels of cybersecurity proficiency for directors above the baseline level of knowledge referenced above.
- Expand and enhance training. As soon as practicable, CISA should work with relevant stakeholders to expand and tailor existing educational offerings for directors to ensure all directors have the recommended baseline level and to help more directors attain higher levels of cybersecurity proficiency.
  - In doing so, CISA should partner with other federal agencies to leverage existing methodologies, programming, and content.
  - For example, CISA could partner with the U.S. Secret Service, which runs a training program for directors at their training facility, the J.J. Rowley Training Center in Beltsville, Maryland. CISA should work with board management software providers to build cybersecurity training/learning/evaluation modules into their platforms.
  - For example, CISA could lead the development of three- to five-minute educational videos and quizzes that are presented within their board software management platforms. Training and educational materials could be delivered as additive, optional offerings within these platforms or could be required, in order for directors to access their board materials. CISA should adapt these offerings for use by non-public company board directors.

- Deliver training at scale. CISA, in coordination with other stakeholders, should encourage and help lead the creation of a centralized cyber education platform, including creating content into which all stakeholders can integrate. This will provide stakeholders with a continuous method for enhancing their cyber literacy.
  - Training opportunities should be delivered at scale and continuously, not just in once-a-quarter or once-a-year posture, and not just when directors access their board materials.
  - Once established, CISA should actively promote educational and training resources and opportunities for board members and CISOs so that these resources are widely known and utilized.
- Promote director certification and accreditation. CISA should encourage the broader adoption of cybersecurity certifications and accreditations like what is offered today by NACD, ISC2 and other stakeholders. NACD's certification includes cybersecurity content aligned with business resilience exposures.
- CISA should use its influence and voice to encourage companies to look for this certification in selecting directors and to weigh the attainment of this certification in their director selections.
- Educate about business imperative. CISA should work with partners to develop quantitative and qualitative analyses demonstrating the relationship between inadequate cybersecurity programs and business and operational risk and by actively and broadly discussing and promoting this concept among all stakeholders.
  - The key to educating and motivating directors lies in demonstrating to directors and management that cyber resilience is a business imperative.
- Expand and enhance training for other stakeholders.
  - More education and training are needed for other stakeholders, especially CISOs, so they can better communicate with directors. Resources are also needed to better educate other stakeholders, including regulators, auditors, insurers, and investors. The training platform described above could be adapted to support the education and training of other types of stakeholders. CISA should study the question and incorporate its findings into future LOEs.
- CISA should work with other relevant federal agencies and stakeholders to generate Principles for Cyber-resilient Investing, the purpose of which shall be to bring cyber resilience to the forefront of investor decision-making. These principles could be modeled after the Principles for Responsible Investment developed in 2006 by an organization affiliated with the United Nations, the purpose of which was to promote the incorporation of environmental, social, and corporate governance factors (ESG) into investment decision-making.[10]

Pillar II: Measurement

The Committee lacks the right data, and even the right methods for collecting such data, to assess how well directors provide oversight to firms on cybersecurity matters. More relevant and accurate data, new data collection methodologies and guidance on recommended best practices are needed in a few key areas. These areas include: 1) Director cyber knowledge, engagement, and effectiveness; 2) Effectiveness of communications between directors and management on cybersecurity matters; 3) Effectiveness of board oversight; and 4) Enterprise cyber risk.

- Identify data deficiencies. CISA should work with other stakeholders to identify areas where data is deficient and to seek new data sources for these.
  - As soon as practicable, CISA should identify areas in which more relevant and accurate data is needed. These areas include, but are not limited to:
    - ➢ Director education, engagement, and effectiveness,
    - ➢ Effectiveness of communications between directors and management on cybersecurity matters,
    - ➢ Effectiveness of board oversight, and
    - ➢ Enterprise cyber risk.
- Measure director engagement. CISA, in collaboration with relevant U.S. agencies, should develop a list of research and data that is necessary to assess directors' level of education and engagement on matters of cybersecurity oversight.

[10] https://www.unpri.org/about-us/about-the-pri

- CISA, in partnership with relevant agencies and stakeholders, should promulgate guidance on how to measure director engagement and director effectiveness in executing their responsibilities.
- Measure the effectiveness of communications. CISA should determine what data and metrics are needed in this area, and then develop guidance on best practices in communications between management and boards, including what level of technical detail and preferred formats and modes for transmission of such information.
- CISA should develop a subset of this guidance as it pertains to directors of non-public companies.
  - Directors must have access to relevant and timely information from management and must be able to use that information to assess cyber risk and performance and, with firm management, implement changes. CISA can weigh in on methods, including platform-based technologies, which some companies find significantly facilitate communications.
- Measure the effectiveness of board oversight. CISA, in partnership with relevant stakeholders, should develop a Framework for Effective Board Oversight.
  - The Framework for Effective Board Oversight (Framework) should describe best practices in board governance and could include recommendations on "governance controls," including how often a board should be briefed by a CISO, how it should structure itself with respect to committees, how it should best utilize insurance products and third-party assessments tools.
  - The Framework should include resources such as exemplary committee charters, lists of common risk factors, approaches for enterprise risk management (ERM), and resolving critical audit matters (CAMs). The Framework could also enumerate and clarify the types of business and financial factors that should be contemplated when determining incident materiality.
  - The Framework should contain methodologies for measuring boards' progress in implementing the Framework, meeting the stated goals stated of its cybersecurity plans, addressing findings and MWs, and increasing the firm's overall operational resilience.
  - In creating the Framework, CISA should draw upon existing work from NACD, DDN, World Economic Forum, and NIST.[11] Eventually, a variant of this Framework should be created for directors of non-public companies.
- Measure enterprise cyber risk.
  - Several proven cybersecurity risk management frameworks exist, but companies are confused and need guidance on which one they should adopt and how to implement it. At the direction of the President, the Office of the National Cybersecurity Director, Office of Management and Budget and Independent and Executive Branch Regulators are in the process of harmonizing baseline cybersecurity requirements for all companies deemed to be part of a critical sector. However, the July 2021 National Security Memorandum (NSM) on Improving Cybersecurity for Critical Infrastructure Control Systems directed CISA and NIST to develop the CPGs, referenced above, and these should serve as the prevailing cybersecurity risk framework all companies should use, especially when no other set of cybersecurity controls is mandated by regulation.
- CISA, in partnership with the White House and SEC, should consider whether corporations should be required to adopt CPGs as the cybersecurity risk management framework against which they must report. This requirement could apply to all publicly traded companies or could apply only to those that are not already required by a U.S.-based regulatory agency to implement a NIST-based set of cybersecurity controls.
- CISA, in partnership with public and private sector stakeholders, should hold a series of workshops demonstrating how companies effectively implement the CPGs or other cybersecurity risk management frameworks.
  - These workshops should showcase examples of how firms measure their progress in implementing such frameworks and how well the implementation of these frameworks contributes to firms' overall cyber resiliency and cybersecurity risk reduction. These workshops should showcase approaches and technologies that allow management and boards to understand the correlation between the implementation of cybersecurity risk frameworks and specific controls to reduce cyber risk.
- Manage risk transfer. CISA should study the criteria used by underwriters in setting cybersecurity insurance

[11] The NIST Cybersecurity Framework 2.0, released on August 8, 2023, contains a new function, "Govern," to cover organizational context; risk management strategy; cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and oversight. https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

policies and establish practices for managing risk via the risk transfer markets to understand the role of risk transfer more accurately in influencing corporate and director behavior and to inform the promulgation of guidance recommended elsewhere in this report.
  - The financial risk resulting from cyberattacks can be managed to some extent by transferring risk via insurance policies. Insurance companies assess firms' cybersecurity risk readily and well.
- Utilize third party assessments. CISA should promulgate guidance that includes best practices and recommendations for how companies can successfully incorporate such capabilities into their cyber risk assessments.
  - Many firms utilize third-party security ratings tools which provide an "outside-in" assessment of how firms are meeting common cybersecurity benchmarks. Directors have increasingly become aware of and may leverage such tools.
- Stay neutral on cyber risk ratings by credit rating agencies. CISA should not encourage credit rating companies to establish ratings of companies' cyber risk.
  - If credit ratings companies develop products aimed at assessing cyber resilience, readiness, or compliance they can provide useful data to directors and managers, but they do not constitute a definitive means of assessing a firm's cyber risk. In June of 2023, the SEC directed all federal agencies to reduce reliance on and references to credit ratings in agency regulations.[12]

Pillar III/Responsibility

We must draw lines of responsibility and accountability for and between stakeholders in key corporate roles, define what is needed to ensure directors are responsible and accountable, and foster stronger and more effective communication and coordination amongst stakeholders.

- Help directors build better understanding of business impact. CISA should create materials that explain the loss and liability to companies for certain types of cybersecurity events.
  - The greatest single factor that will generate more director engagement is to create commonly accepted ways of quantifying and demonstrating the business impact of firms' failure to implement an effective cybersecurity strategy, including adopting a known cybersecurity risk framework. It can do so quantitatively through financial modeling, and it can do so qualitatively by emphasizing the stories and experiences of other companies.
- CISA should create methods for directly linking certain actions and non-actions, as well as investments and failure to invest, to potential cyber risk and then, in turn, communicate that risk in dollar amounts.
- CISA should conduct and publish research on this question and in doing so, should ask the industry to collaborate and provide data.
  - If the cybersecurity risk management frameworks like CPGs, NIST CSF, MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and CIS Top 20 represent the most important controls for companies to implement, then directors must understand how much they reduce their risk by implementing them and how much they increase their risk by not implementing them.
- Generate more relevant and accurate data. CISA should create such a data set and continually update it, with assistance from the Information Sharing and Analysis Centers (ISACs) and the insurance industry.
  - Relating directly to the above and to Pillar III/Measurement, more relevant and accurate data is needed for companies to be able to quantify the business impact of cyber risk. Companies not only need more comprehensive insights into risk across their enterprises preferably in real or near-real time (some companies use network monitoring tools that may provide this, some do not), but they also need sector-wide actuarial data that helps them understand their own risk in the context of their corporate profile.

[12] https://www.sec.gov/news/statement/lizarraga-statement-credit-ratings-060723

- Create Performance Goals for Cyber-Responsible Boards. CISA, in collaboration with relevant stakeholders, should create Performance Goals that contain a set of principles and accompanying best practices for cyber-responsible boards to help directors focus their efforts and attention and help their firms improve cybersecurity outcomes.
    - These Performance Goals should enable directors to view cybersecurity from a position of empowerment rather than fear. CISA should begin this work as soon as practicable, given a reasonable timeline for obtaining the data needed to inform the effort. The Performance Goals should:
        - Define what is an adequate level of training and knowledge for board members on cybersecurity oversight, noting that all members of the board should have some baseline knowledge of and be engaged in cybersecurity matters, not just those serving on relevant committees (overlaps with Pillar I/Board Member Education).
        - Describe board members' core responsibilities pertaining to cybersecurity which, among other things, include approving cybersecurity policies, overseeing cyber risk management, and verifying regulatory compliance.
        - Illustrate examples of well-drawn lines of responsibility and accountability between stakeholders in these roles.
        - Provide examples of how boards can achieve effective communication and coordination among stakeholders.
    - Illustrate variants of board structures that work well for companies, including how management reports to the board and board committees. CCR does not endorse the creation of a cybersecurity committee because it lacks business, operational and financial context which introduces a disconnect between the management team and the broader board membership. CCR does support cybersecurity oversight residing in the risk committee that contains complementary risk domains such as privacy, supply chain and geopolitical. CISA should allow flexibility in its guidance on board structure, especially in recommending what works well for companies of certain sizes and types.
    - Illustrate variants of committee charters that work well for different companies. CISA should partner with relevant federal agencies and other stakeholders to publish an exemplary charter of the committee responsible for cybersecurity oversight, make it a public document and make it flexible enough for different types of companies dealing with different (and changing) regulatory requirements and controls.
    - CISA should create a parallel set of principles and accompanying practices aimed at board directors for non-public companies.
- Create common controls, measurements, and reporting. Consistent with the recommendations included in Pillar II/(Measure enterprise cyber risk), CISA should work with the White House and the SEC to consider whether the CPGs should serve as the prevailing baseline of controls against which determinations of material weaknesses (MWs) and significant deficiencies (SDs) are made for the purposes of SEC reporting, whether for all companies or only for those that are not already required by a U.S.-based regulatory agency to implement a NIST-based set of cybersecurity controls.
    - New SEC cybersecurity rules adopted in July 2023 would require publicly traded companies to disclose a cyber incident within four business days and to provide disclosure in periodic reports about certain cybersecurity governance practices. However, the rules do not include requirements concerning what companies should be doing to increase their cyber preparedness and resilience. Having a common set of cybersecurity controls that all public companies must implement will make it clear what companies must do, as well as create a common set of measurement and reporting methodologies that assess and communicate companies' implementation of the required controls. How determinations of MWs and SDs are made represents the single greatest factor influencing director behavior and therefore firms' overall cyber preparedness and resilience. Directors act to immediately address such findings when they appear, including by making resources available to CISOs.
- Amend CPGs to include flow-down to suppliers and encouragement of secure-by-design. CISA should adapt the CPGs to include, under "Vendor/Supplier Cybersecurity Requirements," questions to suppliers and potential suppliers regarding their board governance practices (to determine how much oversight their boards provide and

how engaged they are on cybersecurity matters) as well as questions about their implementation of a widely accepted cybersecurity risk management framework.
  - Ensuring that the products sold do not cause people harm is a board-level responsibility, demonstrated over many decades and across many industries. Companies that produce hardware and software are not exempted from this responsibility with regard to weaknesses and vulnerabilities in their products that introduce cyber risk to U.S. households and enterprises.
- CISA should adapt the CPGs to include guidance to software and hardware manufacturers to follow the secure-by-design and secure-by-default principles and approaches created by CISA.[13]
- Promote greater use of checklists by auditors. CISA should encourage the inclusion of these broadly and through the CPGs to elicit more board engagement and accountability.
  - Auditors create checklists based on regulatory frameworks, including some of the newer ones described in this report. These checklists can include questions on how boards conduct themselves and how management reports to the board on cybersecurity matters (e.g. "Does your CISO report to the board?" or "Are they a member of an Information Sharing and Analysist Center (ISAC)?").
- Greater clarity on due diligence and liability. In addition to efforts to support the adoption of the CPGs as the common set of controls for publicly traded companies, CISA should create guidance for directors on what constitutes due diligence when it comes to cybersecurity.
- CISA should help define for boards and management the legal frameworks to help them navigate personal and organizational liability issues.
- CISA should simultaneously work with relevant federal agencies and stakeholders to determine what barriers exist to shareholders' pursuing class action lawsuits against companies for weak cybersecurity programs that result in harm to them or their customers.

Pillar IV: Sustained Leadership and Collaboration

Dedicated, high-level CISA leadership and stronger interagency and cross-sector collaboration are needed to augment awareness, knowledge, and governance abilities among the stakeholders of corporate cyber governance. We must foster more regular, authentic stakeholder interaction around the challenges of creating cyber resilient corporations that enhances learning and standards development but provides corporations with tools and information that helps them meet their own unique structures and needs.

- Assign a high-level leader and staff. As soon as practicable, CISA should designate an official under its Cybersecurity Division (CSD) to lead a line of effort around increasing national corporate cyber responsibility.
  - This individual should be high-level and should have previous industry experience, either as a former board member or former CISO reporting to a board. This person shall have, as one of their ongoing responsibilities, the evaluation of CISA's overall efforts relating to corporate cyber responsibilities, as recommended in this report.
  - CISA should assess the number and level of personnel required to implement the accepted recommendations in this report and dedicate these full-time equivalents to this line of effort, reporting to the aforementioned leader. To assist with the LOE, CISA should take advantage of industry expertise by leveraging rotational programs such as the Cyber Innovation Fellows or the Loaned Executive Program.[14]
- Create an awareness campaign.
- CISA should create an awareness campaign to encourage a nationwide culture of corporate cyber responsibility. Through this campaign, CISA should solicit feedback from relevant stakeholders and promote the resources it and its partners have created to foster and enable stronger board engagement.

[13] https://www.cisa.gov/securebydesign

[14] https://www.dhs.gov/loaned-executive-program#:~:text=The%20Loaned%20Executive%20Program%20is,security%20challenges%20through%20the%20Program.

Appendix A: List of Contributors to this Report

The following CCR subcommittee members participated in the study and recommendations documented in this report.

Dave DeWalt, Subcommittee Chair, NightDragon
Vijaya Gadde, Former Twitter
Ron Green, Mastercard
Cathy Lanier, National Football League
Ciaran Martin, Former National Cyber Security Centre
Ted Schlein, Kleiner Perkins
Alex Stamos, Krebs Stamos Group
Kevin Tierney, General Motors
Alex Tosheff, VMware
Chris Young, Microsoft