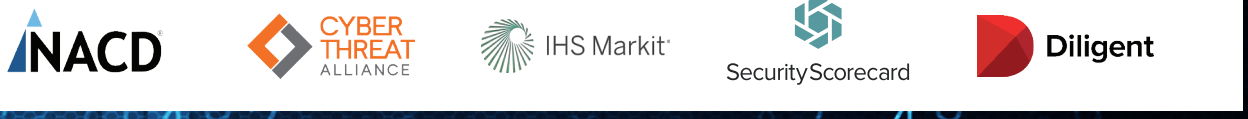
The State of Cyber-Risk Disclosures of Public Companies



March 2021

EXECUTIVE SUMMARY

The U.S. Securities and Exchange Commission (the "SEC," or the "Commission") has in recent years demanded greater transparency from public companies in how they identify, measure, and manage cyber-risk. Too often, cyber-related disclosure language is boilerplate in a way that could not assist an investor in assessing a company's cyber-risk profile or management of those risks.

In the wake of SolarWinds and the increased supply-chain security scrutiny in Washington DC, companies should be explaining to investors the specific risks they face from cybersecurity threats, including, among others, operational disruption, intellectual property theft, loss of sensitive client data, and fraud caused by business email compromises. Companies should also be explaining the categories of both technologies and processes they employ to mitigate those risks. Failure to do so is increasingly costly and is described by former SEC Commissioner Robert J. Jackson Jr. as "the most pressing issue in corporate governance today."

In practice, businesses are slowly but unmistakably moving in the direction of increased transparency. This trend must continue for investors to begin deriving actionable value from cyber-risk disclosures. For example, certain companies are beginning to identify the specific technologies they are using in their program through their cyber-risk disclosures; others have started noting the materiality of their vendor risk exposure, to which regulators are paying particular attention in the aftermath of the 2020 SolarWinds attack. The next logical step is for these evolutions to converge.

An increasing number of tools are available to help companies evaluate their own security posture and that of their partners and vendors. For example, security ratings, as recently recommended by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), can create objective metrics to cover, amongst others, leading cyber hygiene indicators like Domain Name System (DNS) health, web application security, network security, leaked information, endpoint security, and patching cadence.

There are signs Congress may step in. Bipartisan legislation has already been introduced (the Cybersecurity Disclosure Act of 2019) that would direct the SEC to require public companies to disclose board expertise or experience in cybersecurity. Likewise, the Cyberspace Solarium Commission has recommended amending the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7201) to "harmonize and clarify cybersecurity oversight and reporting requirements" for publicly traded companies.

While disclosure regulations are adequate, investors need more specificity about cyber-risk to appropriately manage their market exposure. Companies should articulate what strategies and tools they are using to manage cyber-risk (e.g., incident response planning, deploying available technologies, and using independent or outside-in assessments).

THE STATE OF CYBER-RISK DISCLOSURES OF PUBLIC COMPANIES

By: SecurityScorecard, National Association of Corporate Directors (NACD), Cyber Threat Alliance, IHS Markit, and Diligent

As is evident from its webpage, "*Spotlight on Cybersecurity, the SEC and You*", the SEC continues to focus on both (1) increased cybersecurity risks faced by public companies and regulated entities, and (2) investors' reliance on inadequate cybersecurity risk disclosures. The SEC issued best practices guidance in 2018 for cybersecurity risk disclosures (the "2018 SEC Guidance"), expanding on related guidance from 2011.[1] Likewise, in December 2019, the SEC's Division of Corporation Finance issued staff guidance on the disclosure obligations of public companies with respect to intellectual property and technology risks associated with international business operations, stating:

"[…] we encourage companies to provide disclosure that allows investors to evaluate these risks through the eyes of management. Importantly, disclosure about these risks should be specifically tailored to a company's unique facts and circumstances. In this same vein, where a company's technology, data or intellectual property is being or previously was materially compromised, stolen or otherwise illicitly accessed, hypothetical disclosure of potential risks is not sufficient to satisfy a company's reporting obligations."[2]

The Office of Compliance Inspections and Examinations published ransomware and credential compromise risk alerts in July and September 2020, respectively, in response to an increased number of cyber-attacks against SEC-regulated market and investment intermediary registrants.[3] Gartner has also reported on the "surge in ransomware affecting organizations' operational systems" and supply chains.[4] NACD estimates that 2020 saw seven times more ransomware attacks than 2019, attributable at least in part to vulnerabilities introduced by entire workforces transitioning to a remote work environment in response to the COVID-19 pandemic.[5] Yet even the most damaging of these ransomware events are under-reported in cyber-risk disclosures.

1 Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures", Nos. 33-10459; 34-82746, February 26, 2018, available online at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

2 Guidance issued by the Division of Corporation Finance "is not a rule, regulation or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content." Division of Corporation Finance, Securities and Exchange Commission, "Intellectual Property and Technology Risks Associated with International Business Operations," December 19, 2019, available online at: https://www.sec.gov/corpfin/risks-technology-intellectual-property-international-business-operations.

3 While the Office of Compliance Inspections and Examinations' risk alerts are not rules, regulations, or statements of the SEC, and have no legal force or effect, "the results of [its] examinations are used by the SEC to inform rule-making initiatives, identify and monitor risks and improve industry practices and pursue misconduct." About the Office of Compliance Inspections and Examinations, modified August 26, 2020, available online at: https://www.sec.gov/ocie/Article/ocie-about.html; Office of Compliance Inspections and Examinations, Risk Alert, September 15, 2020, "Cybersecurity: Safeguarding Client Accounts against Credential Compromise", available online at: https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf; Office of Compliance Inspections and Examinations, Risk Alert, July 10, 2020, "Cybersecurity: Ransomware Alert", available online at: sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf.

4 Gartner, press release, "Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025," January 28, 2020, available online at: https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-.

5 C. Hetner and R. Peak, National Association of Corporate Directors, "Cyber Agenda May Affect Liability, Disclosure, and Enforcement," January 26, 2021, available online here: https://blog.nacdonline.org/posts/us-2021-cyber-agenda.

I. THE STATE & ENFORCEMENT OF CYBER-RISK DISCLOSURES

While the SEC and investors view cyber-risk as a priority concern, the average public company's cyber disclosure contains insufficient detail for investors looking to evaluate its risk profile and to understand which remediation strategies, if any, it has implemented to control for the identified risks. Failure to articulate risk and mitigation strategies is increasingly costly: the World Economic Forum reported a 27.4% year-on-year increase in the per-company annual cost of responding to cyberattacks, which averaged £11.7M in 2017 (about USD 15M in 2017 dollars).[6] Former SEC Commissioner Robert J. Jackson Jr. characterized rising cyber threats as "the most pressing issue in corporate governance today," in a March 2018 speech delivered at the Tulane Corporate Law Institute.[7] 79% of the 1,500 global business leaders that participated in the annual 2019 Global Cyber Risk Perception Survey ranked cyber-risk as a top five concern for their organization.[8] Similarly, Gartner's most recent Board of Directors Survey found that "cybersecurity-related risk is rated as the second-highest source of risk for the enterprise," and "few directors [surveyed] feel confident that their company is properly secured against a cyberattack."[9] Certain investors have represented that "given the current environment where cybersecurity attacks are inevitable, they are specifically focused on companies' response and recovery mechanisms," not only whether a company has experienced a cybersecurity incident.[10] And in fact, poor cyber-transparency is said to "undermine investor confidence and negatively impact credit quality," and to "complicate efforts by companies to raise capital and access liquidity."[11]

The SEC has in the past pursued enforcement action against companies that under-disclose or fail to disclose relevant cyber-risks to investors. In 2018, for example, the SEC announced that Altaba Inc. (formerly known as Yahoo!, Inc.) had agreed to a $35 million penalty to settle charges that it misled investors by failing to disclose what was at the time the largest-ever theft of user data, affecting over 500 million user accounts.[12] Yahoo! failed to disclose that it had suffered a breach in every quarterly and annual report it filed for almost two years. Only after entering into an agreement to be acquired by Verizon Communications did it make known that it had suffered a breach in 2014.[13] In October 2018, the SEC investigated nine public company victims of cyber-related fraud—specifically, business email compromises (BECs) involving "spoofed or otherwise compromised electronic communications" that resulted in payments

6 World Economic Forum, "The Global Risks Report 2018", 13th ed., 17 January, 2018, available online at: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf, at 15.

7 Former SEC Commissioner Robert J. Jackson Jr., "Corporate Governance: On the Front Lines of America's Cyber War", March 15, 2018, speech delivered at Tulane Corporate Law Institute, available online at: https://www.sec.gov/news/speech/speech-jackson-cybersecurity-2018-03-15.

8 Marsh and Microsoft, 2019 Global Cyber Risk Perception Survey, September 2019, available online at: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

9 Gartner, press release, "Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025," January 28, 2020, available online at: https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-.

10 Bridget M. Neill, Chuck Seets, and Steve W. Klemash, "Disclosure on Cybersecurity Risk and Oversight", October 17, 2019, Harvard Law School Forum on Corporate Governance, available online at: https://corpgov.law.harvard.edu/2019/10/17/disclosure-on-cybersecurity-risk-and-oversight/.

11 Moody's Investors Service, Research Announcement, "Cybersecurity disclosures vary greatly in high-risk industries," October 3, 2019, available online at: https://www.moodys.com/research/Moodys-Cybersecurity-disclosures-vary-greatly-in-high-risk-industries--PBC_1196854.

12 SEC Press Release, "Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million", April 24, 2018, available online at: https://www.sec.gov/news/press-release/2018-71.

13 Securities and Exchange Commission, In the Matter of Altaba Inc., f/d/b/a Yahoo! Inc., Order Instituting Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933 and Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-desist Order, Section 16, available online at: https://www.sec.gov/litigation/admin/2018/33-10485.pdf.

to accounts controlled by the cybercriminals behind the scheme.[14] The victim companies "may have violated federal securities laws by failing to have a sufficient system of internal accounting controls."[15] While the Commission ultimately decided not to pursue related enforcement actions, it "[deemed] appropriate and in the public interest […] to make issuers and other market participants aware that these cyber-related threats of spoofed or manipulated electronic communications exist and should be considered when devising and maintaining a system of internal accounting controls as required by the federal securities laws."[16]

II. CYBER-RISK DISCLOSURES IN PRACTICE

A 2014 PricewaterhouseCoopers (PwC) report posited that corporate adoption of SEC cybersecurity guidance has "resulted in disclosures that rarely provide differentiated or actionable information for investors."[17] Similarly, scholars have stated that SEC guidance on cybersecurity risk disclosures "fails to resolve the information asymmetry at which the disclosure laws are aimed."[18] The subsequently-published 2018 SEC Guidance aimed at bridging this gap has not had the intended effect of improving cyber-risk disclosures, which remain typically generic and fail to "provide specific information that is useful to investors."[19] Former SEC Commissioner Jackson has described the 2018 SEC Guidance as "rel[ying] heavily on the judgments of corporate counsel to make sure investors get the information they need," stating: "I worry that these judgments have, too often, erred on the side of nondisclosure, leaving investors in the dark—and putting companies at risk."[20]

According to a report published by Moody's Investors Service in 2019, "banks and telecommunications & media companies had the most thorough disclosures, discussing their specific cybersecurity risk management strategies in a fair amount of detail."[21] Other sectors, including healthcare, retail, lodging, health insurance, medical devices, and transportation services, "provide the least amount of information, despite having experienced some of the most well-publicized cyber-attacks to date."[22]

14 Securities and Exchange Commission, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements", October 16, 2018, available online at: https://www.sec.gov/litigation/investreport/34-84429.pdf.

15 Securities and Exchange Commission, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements", October 16, 2018, available online at: https://www.sec.gov/litigation/investreport/34-84429.pdf.

16 Securities and Exchange Commission, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements", October 16, 2018, available online at: https://www.sec.gov/litigation/investreport/34-84429.pdf.

17 PwC US and the Investor Responsibility Research Center, "What Investors Need to Know About Cybersecurity: How to Evaluate Investment Risks", June 2014, available online at: https://www.advisorselect.com/transcript/what-investors-need-to-know-about-cybersecurity-how-to-evaluate-investment-risks/what-investors-need-to-know-about-cybersecurity-how-to-evaluate-investment-risks.

18 Matthew F. Ferraro, "Groundbreaking" or Broken? An Analysis of SEC Cybersecurity Guidance, its Effectiveness, and Implications", 77 Albany L. Rev. 297 (2014).

19 Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures", Nos. 33-10459; 34-82746, February 26, 2018, page 13, available online at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

20 Former SEC Commissioner Robert J. Jackson Jr., "Corporate Governance: On the Front Lines of America's Cyber War", March 15, 2018, speech delivered at Tulane Corporate Law Institute, available online at: https://www.sec.gov/news/speech/speech-jackson-cybersecurity-2018-03-15.

21 Moody's Investors Service, Research Announcement, "Cybersecurity disclosures vary greatly in high-risk industries," October 3, 2019, available online at: https://www.moodys.com/research/Moodys-Cybersecurity-disclosures-vary-greatly-in-high-risk-industries--PBC_1196854.

22 Moody's Investors Service, Research Announcement, "Cybersecurity disclosures vary greatly in high-risk industries," October 3, 2019, available online at: https://www.moodys.com/research/Moodys-Cybersecurity-disclosures-vary-greatly-in-high-risk-industries--PBC_1196854.

Without more detail, SEC registrants' oft-disclosed "risk of experiencing a cybersecurity incident," ultimately weakens the spirit of disclosure: "[i]t is not a question of whether a company will have a [cybersecurity] incident; rather it's a matter of when and how prepared the company is to respond and minimize the impact of the incident."[23] For example, an American multinational hospitality company, in its 10-K for the 2019 fiscal year, disclosed that "[c]yber-attacks could have a disruptive effect on our business," stating further:

"From time to time we and our third-party service providers experience cyber-attacks, attempted and actual breaches of our or their information technology systems and networks or similar events, which could result in a loss of sensitive business or customer information, systems interruption or the disruption of our operations. The techniques that are used to obtain unauthorized access, disable or degrade service or sabotage systems change frequently and may be difficult to detect for long periods of time, and despite our deployment of cyber-attack prevention and detection techniques, we are accordingly unable to anticipate and prevent all data security incidents. We have in the past been subject to cyber-attacks and expect that we will be subject to additional cyber-attacks in the future and may experience data breaches."

Without explaining to investors what the company is doing to prevent and handle an anticipated breach the tone of this and certain other SEC disclosures is resigned—"[e]ven if we are fully compliant with legal standards and contractual or other requirements, we still may not be able to prevent security breaches involving sensitive data." A meaningful level of disclosure lies somewhere past citing abstract cybersecurity risks, and somewhere short of "detailed disclosures that could compromise [a company's] cybersecurity efforts—for example, by providing a 'roadmap' for those who seek to penetrate a company's security protections."[24]

Compare the disclosure above with the following 10-K language filed by a multinational technology company for the fiscal year ended June 30, 2020, which describes the protective technologies the company uses to combat cyber-risks:

"To defend against security threats to our internal IT systems, our cloud-based services, and our customers' systems, we must […] maintain the digital security infrastructure that protects the integrity of our network, products, and services, ***and provide security tools such as firewalls and anti-virus software and information about the need to deploy security measures and the impact of doing so****" (emphasis added).*

The company's description of its defensive approaches to cyber-risk provides a welcome level of detail for the investor looking to gauge its cybersecurity posture—an approach that is reportedly more common amongst European companies than their American counterparts, who instead "appear[] more reliant on insurance to manage the financial impact of cyber risk."[25] Yet it is only a first step towards drafting more useful disclosures, and leaves many

23 PwC US and the Investor Responsibility Research Center, "What Investors Need to Know About Cybersecurity: How to Evaluate Investment Risks", June 2014, page 11, available online at: https://www.advisorselect.com/transcript/what-investors-need-to-know-about-cybersecurity-how-to-evaluate-investment-risks/what-investors-need-to-know-about-cybersecurity-how-to-evaluate-investment-risks.

24 Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures", Nos. 33-10459; 34-82746, February 26, 2018, page 11, available online at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

25 Moody's Investors Service, Research Announcement, "Cybersecurity disclosures vary greatly in high-risk industries," October 3, 2019, available online at: https://www.moodys.com/research/Moodys-Cybersecurity-disclosures-vary-greatly-in-high-risk-industries--PBC_1196854.

other foundational questions unanswered, including whether the company is using technology and processes to, for example, monitor the cybersecurity posture of critical vendors in a meaningful and ongoing way.

Consider, too, the Form 10-K of an American multinational retail corporation for the fiscal year ended January 31, 2020, which contemplates specific ways in which it is exposed to vendor cyber-risk:

"We also utilize third-party service providers for a variety of reasons, including, without limitation, for digital storage technology, content delivery to customers and members, back-office support, and other functions. Such providers may have access to information we hold about our customers, members, associates or vendors."

The language of this disclosure is consistent with the SEC's encouragement that public companies acknowledge the "aspects of [their] business and operations that give rise to material cyber-risks and the potential costs and consequences of such risks, including industry-specific risks and ***third party supplier and service provider risks***"[26] (emphasis added). It is not unusual for public companies to outsource key business processes to improve operational efficiencies. Doing so, however, introduces additional layers of cyber-risk and makes vendor monitoring an imperative, especially where they have access to or process sensitive company data. After all, third-party breaches are one of the most significant cyber threat vectors companies face: according to a January 2020 Ponemon Institute survey, as reported by Security Boulevard, "[i]n the past two years, 53% of organizations have experienced at least one data breach caused by a third party."[27]

In its most recent 10-K, the aforementioned retail corporation at least goes as far as to acknowledge that it is vulnerable to third-party cyber-risk—something many other companies are reticent to do. Of course, mere acknowledgement of third-party risk, without more specificity, is unsatisfactory. Just as the technology company has started to identify the technologies it uses to help mitigate certain threat vectors, companies must also identify the processes they employ to manage third-party risk, whether it is through independent assessment tools to monitor vendors on a continuous basis, or by assessing vendors against their peers by sourcing objective ratings. These facts, if disclosed, demonstrate commitment to reducing cyber-risk in quantifiable ways and helps companies set themselves apart in a bid for investor confidence—and in a way that the SEC is coming to expect. Regulator attention to third party risk has increased in the aftermath of the 2020 SolarWinds attack, particularly with respect to how companies and government entities monitor third-party vendors in their supply chain, deploy third-party software, or grant access to critical information systems. It will be interesting to see how public company users of the compromised SolarWinds Orion product disclose that use and the corresponding cyber risk it has introduced to the company.

An increasing number of tools are available to help companies evaluate their own and their vendors' cybersecurity posture. For example, SecurityScorecard and other security ratings

26 Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures", Nos. 33-10459; 34-82746, February 26, 2018, page 15, available online at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

27 Jingcong Zhao, Security Boulevard, "Automation In Compliance: Why It's a Business Imperative and Where to Start", June 23, 2020, available online at: https://securityboulevard.com/2020/06/automation-in-compliance-why-its-a-business-imperative-and-where-to-start/.

organizations offer cyber-risk ratings on, amongst other metrics, Domain Name System (DNS) health, web application security, network security, leaked information, endpoint security, and patching cadence.[28] To meaningfully assess a company's cyber-risk profile, investors will need to understand if the company is availing itself of best-practice tools. The example disclosures cited herein indicate that companies are beginning to address particular technologies they are using; others have started noting the materiality of their vendor risk exposure. The next logical step is for these evolutions to converge.

III. THE CASE FOR CAUTIOUS OPTIMISM

The latest National Association of Corporate Directors (NACD) public company governance survey ("2019-2020 NACD Survey") reports that 75% of directors believe they are receiving a higher quality of information from management as compared with two years ago.[29] Findings from the EY Center for Board Matters' meta-analysis, based on proxy statements and Form 10-K filings of 76 Fortune 100 companies filed from 2018 through May 31, 2020 ("2020 EY Report"), is also encouraging: cybersecurity risk disclosures are exhibiting a slight trend in increased transparency.[30] The 2020 EY Report revealed that while 100% of the company filings reviewed cite cybersecurity as a risk factor, and 99% cite data privacy, it remains rare for companies to provide more detailed disclosures:

- 16% disclosed the use of an external independent advisor to support management;
- 5% disclosed board engagement with an external independent advisor (an increase of one point each year since 2018);
- 7% "stated that preparedness includes simulations, tabletop exercises, response readiness tests or independent assessments" (up from 3% in both 2019 and 2018); and
- 12% disclosed collaborating with peers, industry groups or policymakers (steady from 2019, and up from 7% in 2018).[31]

According to a January 2020 Gartner press release, by 2025, "40% of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member," up from 10% at the time of publishing, partly as a result of the increased risk deriving from a larger digital footprint during, and likely following, the COVID-19 pandemic.[32]

In 2020, only 17% of the Fortune 100 companies surveyed disclosed management reporting cyber-related issues to the board or relevant board committees at a "frequency of at least annually or quarterly; remaining companies used terms like 'regularly' or 'periodically'," even

28 SecurityScorecard, Security ratings, available at https://securityscorecard.com/product/security-ratings.

29 National Association of Corporate Directors (NACD), "2019-2020 NACD Public Company Governance Survey", available online at: https://corpgov.law.harvard.edu/wp-content/uploads/2020/01/2019-2020-Public-Company-Survey.pdf, at 20.

30 EY Center for Board Matters, "What companies are disclosing about cybersecurity risk and oversight in 2020", August 2020, available online at: https://www.ey.com/en_us/board-matters/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight.

31 EY Center for Board Matters, "What companies are disclosing about cybersecurity risk and oversight in 2020", August 2020, available online at: https://www.ey.com/en_us/board-matters/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight.

32 Gartner, press release, "Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025," January 28, 2020, available online at: https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-.

while the 2018 SEC Guidance explicitly states that "[c]ompanies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder."[33]

There is a clear opportunity here to enhance board oversight. First, by ensuring that internal reporting structures are in place to help normalize cybersecurity as a board-level issue. Second, by regularizing the frequency of such internal reporting and disclosing this cadence as part of the company's cyber-risk disclosures to the SEC. Third, by dispelling the perceived friction between business objectives and management of cyber-risks: the 2019-2020 NACD Survey reports that 61% of directors "would be willing to compromise on cybersecurity to achieve business objectives," while only 28% "prioritize cybersecurity above all else."[34] A balance must be struck between "pursuit of digital innovation, transformation, and ultimately corporate growth," and managing the cybersecurity risks that could impede each of the foregoing objectives.[35] A November 2020 post published on the influential Harvard Law School Forum on Corporate Governance recommends cyber-risk disclosure improvements in, among other areas, boardroom capability and boardroom engagement.[36]

Additionally, Congress is also considering how to improve corporate cybersecurity governance. In the 116th Congress Senator Jack Reed introduced the Cybersecurity Disclosure Act of 2019, which "would direct the SEC to issue final rules requiring a registered public company to disclose in its annual report or annual proxy statement whether any member of its board has expertise or experience in cybersecurity."[37]

Finally, in March 2020 the Cyberspace Solarium Commission, established by Congress to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber-attacks of significant consequences," issued a report including multiple recommendations to improve the cybersecurity of the nation. The Commission recognized that transparency is an important element in improving cyber-risk management. One of its recommendations included amending the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7201) to "harmonize and clarify cybersecurity oversight and reporting requirements for publicly traded companies []," including by mandating that public companies maintain internal records of cybersecurity risk assessments.[38]

33 EY Center for Board Matters, "What companies are disclosing about cybersecurity risk and oversight in 2020", August 2020, available online at: https://www.ey.com/en_us/board-matters/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight; Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures", Nos. 33-10459; 34-82746, February 26, 2018, page 18-19, available online at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

34 National Association of Corporate Directors (NACD), "2019-2020 NACD Public Company Governance Survey", available online at: https://corpgov.law.harvard.edu/wp-content/uploads/2020/01/2019-2020-Public-Company-Survey.pdf, at 5.

35 National Association of Corporate Directors (NACD), "2019-2020 NACD Public Company Governance Survey", available online at: https://corpgov.law.harvard.edu/wp-content/uploads/2020/01/2019-2020-Public-Company-Survey.pdf, at 19.

36 Paul Ferrillo, Bob Zukis, and Christophe Veltsos, "Next-Generation Cybersecurity Disclosures for Publicly Traded Companies", November 4, 2020, Harvard Law School Forum on Corporate Governance, available online at: https://corpgov.law.harvard.edu/2020/11/04/next-generation-cybersecurity-disclosures-for-publicly-traded-companies/.

37 Paul Ferrillo, Bob Zukis, and Christophe Veltsos, "Next-Generation Cybersecurity Disclosures for Publicly Traded Companies", November 4, 2020, Harvard Law School Forum on Corporate Governance, available online at: https://corpgov.law.harvard.edu/2020/11/04/next-generation-cybersecurity-disclosures-for-publicly-traded-companies/.

38 United States of America Cyberspace Solarium Commission, "Introduction", available online at: https://www.solarium.gov/; the Cyberspace Solarium Commission, Final Report, March 2020, available online at: https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxlXJGT4yv/view.

IV. RECOMMENDATIONS AND CONCLUSION

To be clear, current disclosure regulations are adequate but through guidance the SEC has demonstrated its expectation for more meaningful cyber-risk information from public companies. For example, it would be helpful to investors for companies to disclose "cyber-enabled intellectual property theft […] to inform defensive actions at other companies, allow the discovery of larger campaigns," and encourage increased investment in security.[39] Even where theft has not occurred, there are arguments for requiring companies to disclose "the number and type of incidents that occurred in the previous year, […] total spending on cybersecurity and spending as a percentage of information technology spending."[40] To this end, standardizing the definitions of "event," "incident," and "data breach," could be valuable.[41]

Publicly traded companies can balance the need for disclosure without sharing sensitive data in a number of different ways. Most notably by leveraging cyber-risk ratings capable of providing "point-in-time" reports will allow companies to fulfill the aim of the 2018 SEC Guidance and build investor trust without "publicly disclos[ing] specific, technical information about [their] cybersecurity systems, […] in such detail as would make such systems […] more susceptible to a cybersecurity incident."[42] Cyber-risk ratings will also provide a valuable metric upon which a company and its investors will be able to measure progress with regard to its overall cyber health. On January 14, 2021, the U.S. Cybersecurity and Infrastructure Security Agency identified security ratings as a component of cyber-risk metrics, characterizing them as "a starting point for companies' cybersecurity capabilities and [a tool to] help elevate cyber-risk to board decision making."[43]

Businesses are indeed slowly but unmistakably moving in the direction of increased transparency, and as we have seen, are starting to identify their specific mitigation approach to cyber-risk and recognize third party vendors as serious threat vectors. This trend must continue for investors to begin deriving actionable value from cyber-risk disclosures. Gaining investor confidence will depend on companies' willingness to move beyond identifying systemic cyber-risks to articulating which proven strategies and tools they are using to manage them. The SEC expects it and investors deserve it.

39 Robert K. Knake, Council on Foreign Relations Digital and Cyberspace Policy Program, "Expanding Disclosure Policy to Drive Better Cybersecurity", October 16, 2019, available online at: https://www.cfr.org/report/disclosure-policy-cybersecurity.

40 Robert K. Knake, Council on Foreign Relations Digital and Cyberspace Policy Program, "Expanding Disclosure Policy to Drive Better Cybersecurity", October 16, 2019, available online at: https://www.cfr.org/report/disclosure-policy-cybersecurity.

41 Robert K. Knake, Council on Foreign Relations Digital and Cyberspace Policy Program, "Expanding Disclosure Policy to Drive Better Cybersecurity", October 16, 2019, available online at: https://www.cfr.org/report/disclosure-policy-cybersecurity.

42 Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures", Nos. 33-10459; 34-82746, February 26, 2018, page 11, available online at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

43 B. Kolasky, "A Risk-Based Approach To National Cybersecurity," January 14, 2021, available online at: https://www.cisa.gov/blog/2021/01/14/risk-based-approach-national-cybersecurity.