10-2022

A Proposed SEC Cyber Data Disclosure Advisory Commission

Lawrence J. Trautman
Prairie View A&M University, lawrence.j.trautman@gmail.com

Neal Newman
Texas A&M University School of Law, nnewman@law.tamu.edu

A Proposed SEC Cyber Data Disclosure Advisory Commission

*By Lawrence J. Trautman and Neal F. Newman**

Introduction

Public disclosure isn't new. We've been requiring disclosure of important information from companies sincee Great Depression. The basic bargain is this: investors get to decide what risks they wish to take. Companies that are raising money from the public have an obligation to share information with investors on a regular basis. Over the decades, there's been debate about disclosure on things that, today, we consider pretty essential for shareholders.

Today, investors increasingly want to understand the climate risks of the companies whose stock they own or might buy. Large and small investors, representing literally tens of trillions of dollars, are looking for this information to determine whether to invest, sell, or make a voting decision one way or another.

---

*BA, The American University; MBA, The George Washington University; J.D., Oklahoma City University School of Law. Mr. Trautman is Associate Professor of Business Law and Ethics at Prairie View A&M University; Adjunct Faculty, Texas A&M University School of Law (By Courtesy); External Affiliate, Indiana University Bloomington, Ostrom Workshops in Data Management & Information Governance, and Cybersecurity & Internet Governance. Professor Trautman is a past president of the New York and Washington, DC/Baltimore chapters of the National Association of Corporate Directors (NACD). He may be contacted at Lawrence.J.Trautman@gmail.com.

BBA (Accounting) University of Michigan; JD (Banking, Corporate Finance, and Securities Law) Howard University School of Law. Mr. Newman is a CPA and Professor of Law at Texas A&M University School of Law. He may be contacted at nnewman@law.tamu.edu.

The authors wish to extend particular thanks to the following for their assistance in the research and preparation of this article: Anup Agrawal; Kara Altenbaummer-Price; Ross Anderson; John W. Bagby; Stephen Bainbridge; Colleen M. Baker; Dorsey Baskin; Alan L. Beller; Denny R. Beresford; Jody M. Blanke; Marc Blitz; Luigi Bruno; Frederick R. Chang; Jing Chen; Robert M. Chesney; John C. Coffee; Lawrence A. Cunningham; Brian Elzweig; Timothy L. Fort; Cynthia Glassman; Christopher P. Guzelian; Janine Hiller; Kimbery Houser; Asaf Lubin; Mason Molesky; John F. Olson; Peter C. Ormerod; Mauri Osheroff; Jennifer M. Pacella; Robert A. Prentice; Angie Raymond; Scott Shackelford; Marc Steinberg; Kevin Werbach; James Wetherbe; and Arthur E. Wilmarth. Thanks also to Gary Marchant and all those responsible for the 9th Annual Governance of Emerging Technologies and Science Conference, May 19–20, Sandra Day O'Connor College of Law, Arizona State University. All errors and omissions are our own.

Gary Gensler
Chairman, Securities and
Exchange Commission
July 28, 2021[1]

Constant cyber threats result in: intellectual property loss; data disruption; ransomware attacks; theft of valuable company intellectual property and sensitive customer information. Cyber attacks disrupt the very flow of reliable information and thought in a democratic society, threatening free speech and other necessary Constitutional provisions and guarantees.[2] To paraphrase Lord Kelvin's famous observation, "you can't manage what you don't measure."[3] How then does the Securities and Exchange Commission (SEC) craft a disclosure regime that captures in a structured data format all those measurable components of costs that allows management and investors to better understand the true costs incurred in cyber defense and breach mediation? This inquiry logically dovetails into the broader question of externality costs associated with cyberattack that, when ignored by industry, are placed as additional burdens upon government and other institutions (such as municipalities, school systems and universities) and consumers when their identity data is stolen and fraud subsequently committed against them. SEC chair Gary Gensler states, "The economic cost of cyberattacks is estimated to be at least in the billions, and possibly in the trillions, of dollars. Hackers have attacked broker-dealers, governmental agencies, meat processors, and pipelines. These attacks can take many forms from denials-of-service to malware to ransomware."[4] By now, a broad understanding of the pervasive threat of cyberattack from international criminal organizations, nation states, and even poorly capitalized criminal elements are legion.[5] We will not replicate that discussion here, except to briefly mention several recent attacks to illustrate some of the difficulties and challenges in capturing accurate aggregate cost data. We commend the SEC for their March 2022 issuance of a proposed rule addressing Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,[6] to require:

1. Current reporting about material cybersecurity incidents;
2. Periodic disclosures about a registrant's policies and procedures to identify and manage cybersecurity risks;
3. Management's role in implementing cybersecurity policies and procedures;
4. Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk;

5. Registrants to provide updates about previously reported cybersecurity incidents in their periodic reports; and
6. Cybersecurity disclosures to be presented in Inline extensible Business Reporting Language ("Inline XBRL").[7]

This paper was submitted as a recommendation in response to the SEC's request for comment to the proposed Rule and submitted on May 9, 2022.[8]

Proposed Cyber Data Disclosure Advisory Commission

In the following pages we recommend that the SEC build upon the March 2022 proposed rule by creating a Cyber Data Disclosure Advisory Commission to be comprised of relevant stakeholder groups to investigate and promulgate suggestions for a standardized disclosure regime for cyber data. Our task of creating a template that will define and capture those measurable costs that are necessarily required for a meaningful analysis is multifaceted. Just a few of the many complex issues include:

1. What cybersecurity disclosure information is useful to investors?;
2. What investments in cyber defense are period costs?;
3. Which costs should appropriately be capitalized such as secondary data recovery centers (if any) and amortized over what period of time (for reporting purposes)?;
4. How do we measure known losses?
5. Which imputed costs (if any), such as lost sales, are appropriate for inclusion in our measurement?
6. Can agreement be reached about how reputational costs associated with cyber breaches should be measured (imputed)?

Our paper proceeds in seven parts. First, we provide a brief discussion about the difficult challenges associated with capturing cyber threat data. Second, is a brief history of the SEC disclosure regime. Third, we address the economics of cybersecurity. Fourth, we provide a proposed schematic for composition and workflow for an SEC Cyber Data Disclosure Commission. Fifth, we highlight the important implications of this study for the preservation of U.S. national security interests. The American business community is a critical link in the national cyber security equation. Any weak link in the system constitutes an unacceptable vulnerability for all citizens. Sixth, we recommend the Commission consider asking Congress to pass legislation creating a Public Company Cybersecurity Oversight Board for publicly-traded companies similar to the PCAOB. And last, we conclude. We believe this proposal is significant and represents a timely contribution in fostering better cooperation between all interested stakeholders in cyber hygiene and security.

I. CHALLENGES OF CAPTURING CYBER THREAT DATA

The SEC's March 2022 issuance of a proposed rule addressing Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure states, "where possible, we have attempted to quantify the benefits, costs, and effects on efficiency, competition, and capital formation expected to result from the proposed amendments. In many cases, however, we are unable to quantify the potential economic effects."[9] Herein lies the problem and the basis for the contribution made by this paper. The SEC acknowledges that:

> [W]e lack information necessary to provide a reasonable estimate. Where we are unable to quantify the economic effects of the proposed amendments, we provide a qualitative assessment of the potential effects and encourage commenters to provide data and information that would help quantify the benefits, costs, and the potential impacts of the proposed amendments on efficiency, competition, and capital formation.[10]

Not only do regulators need this granular information to formulate effective policy, but management, directors, and investors need structured data presented in a meaningful and comparable format to facilitate decisions about this critically important issue. This proposal presents a schematic to achieve just that.

Many Successful Infiltrations Undetected

By now, it is likely that essentially all organizations possessing valuable information have been successfully penetrated by outside entities. In many cases the data architecture of breached entities has successfully been explored and mapped. Former National Security Agency (NSA) director of research Frederick R. Chang has observed, "generally, there are two only types of companies: those that know they have been breached, and those that don't know they have been breached."[11]

Externalities Abound

Examples of cyber breaches abound of situations presenting difficult-to-define aggregate cost scenarios. For example, when an airline experiences a data breach that results in flight cancellations, the airline knows how many flights have been cancelled, passengers rebooked on their later flights, and revenue lost forever when passengers take other carriers. Economists would also suggest that impacted passengers, as a result, likely incur costs associated with missed connections, absences from important meetings, unreimbursed unexpected lodging and meal expenses, loss of productive time, etc. Customer loyalty is a very valuable asset to an airline. Should data breaches happen more than once, passengers may change their affiliation loyalty.

In the case of data breaches resulting in the loss of personally identifiable information (PII) such as the Target breach during 2013,[12] Mariott (2019),[13] or Yahoo (2013),[14] all these companies incurred costs resulting from these breaches. However, many of their customers also incurred unreimbursed expenses as a direct result of these breaches, if only in terms of the lost time and expense associated with mitigating adverse credit reporting events. Congress has recently conducted multiple hearings aimed at understanding the adverse impact of nation state supported actors in fraudulently hijacking social media platforms for use as propaganda proxies.[15] We suggest that this is not without serious costs to our society.

History of Poor Cyber Threat Information

Our history of failed cyber risk management is punctuated with poor information security cost data. Professor Tyler Moore points to the misaligned enterprise incentives that are pervasive in our experience. Consider how, "Information systems are prone to fail when the person or firm responsible for protecting the system is not the one who suffers when it fails. Unfortunately, in many circumstances online risks are allocated poorly."[16] For example, Professor Moore states:

> There is an incentive to under-report incidents across the board. Banks do not want to reveal fraud losses for fear of frightening away customers from online banking; businesses do not want to co-operate with the police on cyber-espionage incidents because their reputation (and their stock price) may take a hit; operators of critical infrastructures do not want to reveal information on outages caused by malicious attack for fear it would draw attention to systemic vulnerabilities. The reticence to share information is only countered by the over-enthusiasm of many in the IT security industry to hype threats.[17]

Consider that, "Systems often fail because the organizations that defend them do not bear the full costs of failure."[18] Your authors contend that a necessary very first step in achieving national cybersecurity for all interested stakeholders is to devise a template for the analysis and better understanding of actual costs. In the absence of widespread understanding, no useful cost-benefit analysis can be conducted with subsequent mitigation of risk.

Definitions

We remain indebted to the Commission for defining the terms "cybersecurity incident," "cybersecurity threat," and "information systems" in their proposed rule announced during March 2022.[19] Accordingly, propose Item 106 and proposed Form 8-K Item 1.05 provide that:

- *Cybersecurity incident* means an unauthorized occurrence on

or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein;

- *Cybersecurity threat* means any potential occurrence that may result in, an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.
- *Information systems* means the information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

What constitutes a "cybersecurity incident" for purposes of our proposal should be construed broadly and may result from any one or more of the following: an accidental exposure of data, a deliberate action or activity to gain unauthorized access to systems or to steal or alter data, or other system compromises or data breaches.[20]

II. THE SEC DISCLOSURE REGIME

"Innovation doesn't come just from updating software and hardware; it also comes from the manner in which products are offered . . . Beyond the innovations and technologies, our economy is changing in other ways. Today, investors are demanding additional information from companies beyond what they've sought historically, with respect to climate risk, human capital, and cybersecurity risk . . .

Again, 'no regulation can be static in a dynamic society.'"

Gary Gensler
Chair
U.S. Securities and Exchange Commission
January 19, 2022[21]

Disclosure of material items is at the very cornerstone of U.S. capital formation and securities regulation. SEC Chair Gary Gensler states, "We have a key role as the regulator of the capital markets with regard to SEC registrants — ranging from exchanges and brokers to advisers and public issuers. Cyber relates to each part of our three-part mission, and in particular to our goal of maintaining orderly markets."[22] In addition, the Commission has, "many rules that implicate cyber risk, including but not limited to business continuity, books and records, compliance,

disclosure, market access, and antifraud. Our Division of Examinations (EXAMS) has put out various Risk Alerts and statements regarding cybersecurity topics and issued a report in 2020 on Cybersecurity and Resiliency Observations."[23] Chairman Gensler states that the work of the Commission assists both SEC registrants and the public in preparation for and management of these cyber risks.[24]

History

In Professor Newman's co-authored Article with Professor Lawrence Trautman, he outlines the historical underpinnings of the current US disclosure regime for publicly traded companies.[25] In that writing, Professor Newman notes that the current disclosure regime governing the buying and selling of securities was spawned during the early part of the 1900's. Recall the great depression and the collapse in the stock market that occurred in 1929.[26] From these events, government recognized that a more formal process needed to be put in place regarding the buying and selling of ownership in companies. The history surrounding the first federal securities law act is a storied one. In fact, it took two attempts before congress had an act it was willing to move forward with.[27]

The first attempt failed due to the initial act's ideological focus. Instead of the informed disclosure regime that we now have, the first attempt was based off of what is referred to as "merit regulation." Merit regulation is an approach that would require regulators in essence to pick stock winners and losers; a speculative endeavor at best and one fraught with what are now clear problematic pitfalls that would result if the government was in the business of deciding which stocks may be worthy and which stocks may be unworthy for public consumption.[28]

Regarding the second attempt. "Harvard law professor (and future Supreme Court Justice) Felix Frankfurter was called in to develop a revised bill. Frankfurter's team including James Landis, Benjamin Cohen, and Tommy Corcoran drafted a bill following the British securities law approach, based primarily on full disclosure of material information leaving it to investors rather than the government to judge the merits of any stock offer."[29] For political reasons, Frankfurter's team decided to start with the failed first draft to use as the basis for drafting the piece of legislation that has stood the test of time and is substantively the same document that was drafted some 88 years ago. As the story is told, Frankfurter's team penned the Securities Act of 1933 over a weekend. To this day, scholars still marvel at the '33 Act's idiosyncratic nature. The Act has been described as "*a masterpiece,*"[30] "*a writing with interwoven complexities and neatly hidden traps,*,[31] "*an intellectual Tour de Force,*"[32] "*a complex*

mental game derived by three exceptional minds."[33] The authors can attest that the Act is unique in the way it is constructed; it is all that it is referred to and more.

Although the '33 Act as penned back in the early 1930's, is idiosyncratic and complex in its drafting, the '33 Act's underlying premise is a simple one: that investors receive full and fair financial disclosure when companies initially issue stock to investors. Likewise, the Exchange Act of 1934 steps in where the '33 Act leaves off and requires full and fair disclosure of publicly traded companies on a periodic and ongoing basis. The idea being, that investors will have access to company information that is readily available for use in making investment decisions.

Much has been written over the years documenting the many spectacular failures in corporate governance[34] and recommending steps to be taken for improvement.[35] We will not attempt to replicate these here.

Sommer 1977 SEC Advisory Committee on Corporate Disclosure

A.A. "Al" Sommer served a three-year term as SEC Commissioner during the 1970s, and thereafter was Chair "for 13 years of the Public Oversight Board, created by the American Institute of Certified Public Accountants to help monitor accounting firms that audit public corporations."[36] As Chair of the SEC's 1977 Advisory Committee on Corporate Disclosure, attorney and professor Sommer stated, "Very simply put . . . if every instance of adultery had to be disclosed, there would probably be less adultery."[37] In explaining the Advisory Committee's report, Chairman Sommer stated:

> [T]he Committee recognized that in any society needs and demands will exceed available resources. When that is the case, as it universally is, it is necessary that the scarce resources be allocated. It is axiomatic that such allocation will be best achieved if those involved in allocation decisions have the benefit of reliable, timely and sufficient information. Thus, in making investment decisions, investors are likeliest to make efficient allocations of resources if they have available information with those characteristics.[38]

Whether they like it or not, recognize it or not, many parties having various roles in the capital formation process (brokers, dealers, corporate management and board directors, investment bankers, venture capitalists, external auditors, and software and data service providers) are unwillingly drawn into the common fight to ensure cybersecurity. The corporate governance literature is full of articles having a focus on privacy[39] and cyber risk.[40] SEC Commissioner Paredes states:

> By ensuring that investors have the information they need to make informed decisions, mandatory disclosure, in turn, leverages market discipline as a means of accountability that obviates the need

> for more substantive government regulation of securities-related activities. Through their investment decisions, investors are able to bring pressure to bear on directors, officers, investment advisers, broker-dealers, and other market participants to serve investor interests. Market participants are incentivized to satisfy investor demands because investors "reward" and "punish" by how and with whom they choose to invest and transact . . . as a regulatory mechanism, disclosure privileges investor choice, favors private ordering over one-size-fits-all mandates, and encourages innovation and competition.[41]

Climate and ESG Task Force Announced

Demonstrating the recent focus and priority of Environmental, Social, and Governance (ESG), on March 4, 2021 the SEC announced the creation of a Climate and ESG Task Force within the Division of Enforcement.[42] Led by Acting Division of Enforcement Deputy Director Kelly L. Gibson, the new task force is "a Division-wide effort, with 22 members drawn from the SEC's headquarters, regional offices, and Enforcement specialized units."[43] The Commission states:

> Consistent with increasing investor focus and reliance on climate and ESG-related disclosure and investment, the Climate and ESG Task Force will develop initiatives to proactively identify ESG-related misconduct. The task force will also coordinate the effective use of Division resources, including through the use of sophisticated data analysis to mine and assess information across registrants, to identify potential violations.
>
> The initial focus will be to identify any material gaps or misstatements in issuers' disclosure of climate risks under existing rules. The task force will also analyze disclosure and compliance issues relating to investment advisers' and funds' ESG strategies. Its work will complement the agency's other initiatives in this area, including the recent appointment of Satyam Khanna as a Senior Policy Advisor for Climate and ESG. As an integral component of the agency's efforts to address these risks to investors, the task force will work closely with other SEC Divisions and Offices, including the Divisions of Corporation Finance, Investment Management, and Examinations. "Climate risks and sustainability are critical issues for the investing public and our capital markets," said Acting Chair Allison Herren Lee.[44]

Laws and regulations are constantly in a race to keep up with rapidly changing technological developments.[45] For example, during mid-February 2022, *The Wall Street Journal* reported, "federal regulators are closing in on rules requiring all public companies to disclose their greenhouse-gas output. But they are struggling to figure out how much detail to demand about emissions produced by businesses' suppliers and customers."[46] According to financial market journalists, it appears that, "SEC officials drawing up the landmark rules face a balancing act. Many inves-

tors are demanding the information so they can judge the risks faced by companies from climate change and regulations designed to mitigate it."[47] Just like climate issues, the governance of cybersecurity can now be recognized as an integral part of ESG—-the "governance" part.[48]

Increased Importance of Cyber Recognized by SEC

Continued recognition of the increased role of cyber security in corporate risk management is observed by the SEC's announcement on May 3, 2022, of "the allocation of 20 additional positions to the unit responsible for protecting investors in crypto markets and from cyber-related threats. [This] newly renamed Crypto Assets and Cyber Unit (formerly known as the Cyber Unit) in the Division of Enforcement will grow to 50 dedicated positions."[49] The SEC states:

> Since its creation in 2017, the unit has brought more than 80 enforcement actions related to fraudulent and unregistered crypto asset offerings and platforms, resulting in monetary relief totaling more than $2 billion. The expanded crypto assets and Cyber Unit will leverage the agency's expertise to ensure investors are protected in the crypto markets, with a focus on investigating securities law violations related to:
>
> - Crypto asset offerings;
> - Crypto asset exchanges;
> - Crypto asset lending and staking products;
> - Decentralized finance ("DeFi") platforms;
> - Non-fungible tokens ("NFTs"); and
> - Stablecoins.
>
> In addition, the unit has brought numerous actions against SEC registrants and public companies for failing to maintain adequate cybersecurity controls and for failing to appropriately disclose cyber-related risks and incidents. The Crypto Assets and Cyber Unit will continue to tackle the omnipresent cyber-related threats to the nation's markets. 'Crypto markets have exploded in recent years, with retail investors bearing the brunt of abuses in this space. Meanwhile, cyber-related threats continue to pose existential risks to our financial markets and participants,' said Gurbir S. Grewal, Director of the SEC's Division of Enforcement.[50]

History of Electronic Disclosure: The EDGAR Releases

Development of an electronic disclosure system began in 1983, with a pilot system opened during fall 1984 for volunteer filings with both the Division of Investment Management and Division of Corporation Finance.[51] "An evaluation of these filings was conducted by the staff between January 1 and June 30, 1994, resulting in a positive assessment of the EDGAR system."[52] The Commission by early 1993 began to require, "electronic filings through it's Electronic Gathering, Analysis, and Retrieval system,

EDGAR. This system is intended to benefit electronic filers, enhance the speed and efficiency of SEC processing, and make corporate and financial information available to investors, the financial community and others in a manner of minutes."[53] In sum, the Commission recognized that, "Electronic dissemination generates more informed investor participation and more informed securities markets."[54] The EDGAR filing system now "requires that official documents—attached to electronically submitted filings—be formatted as one of the following; HTML, American Standard Code for Information Interchange (ASCII), or, whenever specific criteria are met, Portable Document Format (PDF)."[55]

Extensible Business Reporting Language (XBRL)

Now used worldwide by financial regulatory agencies, in recognition of the need for structured automated data analysis, during 2009 the SEC first required issuer submission of data in Extensible Business Reporting Language (XBRL) format; "in a separate XML file or more recently embedded in quarterly and annual HTML reports as inline XBRL . . . [these] facts must be associated for a standard US-GAAP or IFRS taxonomy. Companies can also extend standard taxonomies with their own custom taxonomies."[56] The filer submission histories and XBRL financial statement data currently included in Application Programming Interfaces (APIs) currently include forms 10-K, 10-Q, 8-K, 40-F, 20-F, 6-K and their variants.[57] Incorporation of this structured data schematic, "ensures that facts have a consistent context and meaning across companies and between filings and are comparable between companies and across time."[58] The SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure proposed rule announced during March 2022 provides that registrants be required:

> [T]o tag information specified by Item 1.05 of Form 8-K and Items 1.06 and 407(j) of Regulation S-K in Inline XBRL in accordance with Rule 405 of Regulation S-T (17 CFR 232.405) and the EDGAR Filer Manual. The proposed requirements would include block text tagging of narrative disclosures, as well as detail tagging of Quantitative amounts disclosed within the narrative disclosures. Inline XBRL is both machine-readable and human-readable, which improves the quality and usability of XBRL data for investors.
>
> Requiring Inline XBRL tagging of the disclosures provided pursuant to these disclosure items would benefit investors by making the disclosures more readily available and easily accessible to investors, market participants, and others for aggregation, comparison, filtering, and other analysis, as compared to requiring a non-machine readable data language such as ASCII or HTML. This Inline XBRL tagging would enable automated extraction and analysis of the granular data required by the proposed rules, allowing

> investors and other market participants to more efficiently perform large-scale analysis and comparison of this information across registrants and time periods. For narrative disclosures, an Inline XBRL requirement would allow investors to extract and search for disclosures about cybersecurity incidents reported on Form 8-K, updated information about cybersecurity incidents reported in a registrant's periodic reports, a registrant's cybersecurity policies and procedures, management's role in assessing and managing cybersecurity risks, and the board of directors' oversight of cybersecurity risk and cybersecurity expertise rather than having to manually run searches for these disclosures through entire documents. The Inline XBRL requirement would also enable automatic comparison of these disclosures against prior periods, and targeted artificial intelligence/machine learning assessments of specific narrative disclosures rather than the entire unstructured document. At the same time, we do not expect the incremental compliance burden associated with tagging the proposed additional information to be unduly burdensome because registrants subject to the proposed tagging requirements are for the most part subject to similar Inline XBRL requirements in other Commission filings.[59]

Regulation Systems Compliance and Integrity (Reg SCI)

Speaking during January 2022, SEC Chair Gary Gensler states, "I believe we have an opportunity to freshen up Regulation Systems Compliance and Integrity (Reg SCI).[60] Adopted during 2014, Reg SCI "covers a subset of large registrants, including stock exchanges, clearinghouses, alternative trading systems, self-regulatory organizations (SROs) and the like — financial infrastructure that is part of the backbone of the capital markets."[61] In addition, "The Consolidated Audit Trail (CAT), as a facility of each of the participant SROs, also is subject to Reg SCI."[62] Chairman Gensler adds:

> The rule helps ensure these large, important entities have sound technology programs, business continuity plans, testing protocols, data backups, and so on. The core goal of Reg SCI was to reduce the occurrence of systems issues and improve resiliency when they do occur.
>
> A lot has changed, though, in the eight years since the SEC adopted Reg SCI. Thus, I've asked staff how we might broaden and deepen this rule. For example, might we consider applying Reg SCI to other large, significant entities it doesn't currently cover, such as the largest market-makers and broker-dealers? To that end, in 2020, the Commission proposed to bring large Treasury trading platforms under the SCI umbrella. At our next Commission meeting, we will consider whether to re-propose this rule. Similarly, I think there might be opportunities to deepen Reg SCI to further shore up the cyber hygiene of important financial entities.[63]

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

The SEC's March 2022 issuance of a proposed rule addressing

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure has resulted in both substantial comments received by the Commission,[64] and coverage and commentary in the financial press.[65] Examples of information useful to investors, and all other stakeholders including those who are responsible for securing America's national security, is described by *The Wall Street Journal* when they write, "Under proposals from the SEC, the agency expects to know more about how listed companies manage cyber risk. Businesses would be required to disclose which board directors have cybersecurity expertise, how often the topic of cybersecurity is discussed and what, if any, oversight the board has over cyber matters."[66] Outside the SEC:

> Others say [the proposed rule] provides much needed clarity on expectations from watchdogs, as cybersecurity has become a core business risk for companies.
>
> 'I think it's a reset, and I think the advantage of this reset is they are being very clear. They're telling you what they expect,' said Cyrus Vance Jr., partner and global chair of law firm Baker McKenzie LLP's cybersecurity practice. In practice, security chiefs say, this means that chief information security officers and others with cyber responsibilities must learn how to translate cybersecurity data into clear risk information that nontechnical board directors can quickly understand.
>
> This may force some companies to rethink the role itself, said Shaun Marion, CISO at fast-food chain McDonald's Corp. He said when he landed his first cybersecurity executive position in 2011, he lacked experience interacting with a corporate board and didn't get much help. 'My first board meeting was sink or swim,' he said. 'I wouldn't say I swam.'
>
> The SEC's call for senior leaders and directors to understand and disclose more about their company's cyber-security posture will require a strong relationship between the CISO and the board, he said. 'It will change how we develop the next generation of CISOs,' he said, relying less on technical knowledge and more on business-risk experience . . .
>
> Installing directors with cybersecurity expertise can help the rest of the board grasp these issues, said Baker McKenzie's Mr. Vance.[67]

University of Texas law professor Henry T.C. Hu served as the founding Director of the SEC's Division of Risk, Strategy, and Financial innovation from 2009–2011 (now renamed Division of Economic and Risk Analysis). Professor Hu observes that:

> Since the depression, the federal government's totemic philosophy as to markets and corporations has been to help ensure a robust informational foundation for private decision makers. The rationale was that a disclosure regime center posted by the U. S. Securities and Exchange Commission would contribute to informed choices by market participants, furthering efficiency both in the paper economy and in the real economy. Moreover, this informational foundation would enhance corporate governance. Managements

> would be deterred from behavior unsustainable in the light of day, and the monitoring and disciplining of managements by shareholders, as well as the market for corporate control, would be facilitated . . .
>
> [T]his philosophy was also decidedly incrementalist. The SEC would not venture beyond the realm of information to that of substantive decision making. In the paper economy, the nature and characteristics of the securities offered, the relationships between underwriters and issuers, and the securities' offering and trading prices were left to participants and overall market forces. In the real economy, corporate managements would generally be left to make their own decisions as to the deployment of resources, including in the critical area of risk taking. This philosophy stemmed . . . from Louis Brandeis's deep-seated, compellingly expressed belief in the power?and sufficiency?of bringing sunlight to markets.[68]

Professor Hu contends that the SEC's "disclosure philosophy and its longstanding implementation methodology . . . are at the brink of metamorphosis . . . A new implementation methodology, rooted in a more comprehensive conception of information and facilitated by innovations in computer and Internet technologies, could help address such disclosure challenges."[69] Now, approximately 90 years following creation of the SEC, it seems clear that the "disclosure paradigm emerged in a simpler time, relied on a simple conception of information and implementation strategy, and was directed at simple goals. The modern process of financial innovation . . . [is] far more complex than in the past."[70] Professor Hu writes:

> [I]n order to meet the disclosure and other regulatory challenges posed by financial innovation, it is essential that there not only be enough talented traditional lawyers at the SEC, but that there also be enough talented personnel with other skills and backgrounds. A vigorously interdisciplinary approach, enhanced by 'local knowledge' of market realities, is essential to the formulation of public policy in respect of modern capital markets . . .
>
> To remain vital, the SEC disclosure paradigm must be able to encompass in a meaningful and systematic way the vast complexities of modern markets and institutions. A fundamental and comprehensive rethinking is essential.[71]

III. THE ECONOMICS OF CYBERSECURITY

Rapidly Changing Technological Advances

The challenge of regulating cyber security is hampered by the constantly expanding development of new and disruptive technologies. For example, in just a little over a decade, development of blockchain-based technologies has created many new challenges for the SEC. Multinational criminal organizations have used virtual currencies to pay for the fruits of illegal items and activities. Regulators struggle to understand and craft new

schematics to regulate: virtual currencies, distributive autonomous organizations (the "DAO"), and non-fungible tokens (NFTs), just to name a few. Just around the corner may be novel challenges to securities regulation presented by "deep fake" technology where, "Technologies for altering images, video, or audio (or even creating them from scratch) in ways that are highly-realistic and difficult to detect are maturing rapidly . . . and [will] generate significant policy and legal challenges."[72] Disruption to the U.S. securities regulation process may also result from advances in Quantum Computing developments.[73]

Professors Bushman and Smith discuss "the classic agency perspective that the separation of corporate managers from outside investors involves an inherent conflict. Corporate control mechanisms are the means by which managers are disciplined to act in the investors' interest."[74] Accordingly, outside investors are protected from expropriation by corporate insiders by "control mechanisms [that] include both internal mechanisms, such as managerial incentive plans, direct monitoring, and the internal labor market, and external mechanisms, such as outside shareholder or debtholder monitoring, the market for corporate control, competition in the product market, the external managerial labor market, and securities laws."[75] Elsewhere, Professor William J. Magnuson proposes a "Unified Theory of Data," to "set forth harmonized and consistent rules for the gathering, storage, and use of data, and [to] establish rules to incentivize beneficial data practices and sanction harmful ones."[76] We believe this proposal deserves serious consideration; but, further comment here is beyond the scope of these remarks.

Role of Corporate Directors in Cybersecurity Governance

It is a duty and responsibility of corporate directors to govern cybersecurity and cyber risk.[77] Publicly traded corporations have a duty to disclose the existence of a data breach based upon at least two distinct authorities: Delaware common law and the SEC's 2011 corporate finance disclosure guidance, which identifies material data security risks that companies must disclose under securities law disclosure requirements and accounting standards.[78] Accordingly, companies that know about a data breach but fail to disclose it to shareholders, regulators, and consumers, risk potential liability under corporate, breach notification, and securities laws.

Well established in Delaware common law is the concept that directors' and officers' of a corporation have a fiduciary duty to shareholders and the corporation of disclosure—sometimes referred to as a duty of complete candor.[79] Many years ago, Professor Lawrence A. Hamermesh noted that Delaware courts have recognized "that a fiduciary duty to disclose all material informa-

tion arises when directors approve any public statement, such as a press release, regardless of whether any specific stockholder action is sought."[80]

As early as January 2017, the World Economic Forum in collaboration with The Boston Consulting Group and Hewlett Packard Enterprise issued their Future of Digital Economy and Society System Initiative titled, "Advancing Cyber Resilience: Principles and Tools for Boards."[81] Accordingly, the World Economic Forum writes:

> Countering cyber risk presents a significant strategic challenge to leaders across industries and sectors but one that they must surmount in order to take advantage of the opportunities presented by the vast technological advances in networked technology that are currently in their early stages. Over the past decade, we have significantly expanded our understanding of how to build secure and resilient digital networks and connected devices. However, board-level capabilities for strategic thinking and governance in this area have failed to keep pace with both the technological risks and the solutions that new innovations provide.[82]

Professor and former National Security Agency (NSA) Director of Research Frederick R. Chang warns:

> Basically, what directors need to know about cyber is that it is a strategic risk and not just an IT thing. It's easy to think of it as if, there are some routers or some switches or some firewalls that get broken, resulting in exposed data—- creating a problem. It's important to step back and reflect upon how cyber is a risk, like any other risk. It can be thought of like an earthquake, or a flood or a fire. Much like an earthquake, flood or fire — you can't do anything about it if there's going to be an earthquake and you are located in California. You can't stop the earthquake. All too often, it seems, there is a perception that cyber threat can actually be stopped. It can't be stopped. If a persistent attacker has a really high desire to break through, then they're going to get through. You can't stop them—- and cyber has to be viewed as a risk, like any other risk . . . there are some things you can do to mitigate it the risk, but you can't eliminate the risk Maybe you can buy insurance, you can bring in some more people to work on cybersecurity, and so forth. But cyber threat is fundamentally something you can't stop and it needs to be viewed at that level. So; what steps does a board take to have enough intrinsic knowledge about cyber? The task can be a highly technical thing, but it isn't only a technical concern.[83]

About two decades ago Professors Bushman and Smith crafted a very useful schematic illustrating: "three channels through which financial accounting information may affect economic performance [observing] Governance role of financial accounting information operates through channel 2" (Figure 1);[84] and "predicted interactions between financial accounting regimes and other factors in affecting economic performance" (Figure 2).[85] We have included these usefil diagrams as an Appendix to this document.

The Allocation of Costs

The allocation of costs incurred in cybersecurity efforts is far from a straightforward task. While cybersecurity expenses paid for cyber insurance, or to a consulting firm may seem easy to identify, what portion of corporate information technology expenses should rightfully be included in this calculation? What criteria should be agreed upon so that resulting measurements are comparable across industries? What portion of a secondary data backup facility should be attributed, if any, to cyber risk management?

Professors Wolff and Lehr write that an estimate of total costs for any given data breach incident must, "consider the costs incurred by all market participants, which includes both the parties directly involved, as well as the costs that spillover onto other market participants."[86] In addition:

> Some of the costs to victims show up as revenues to InfoSec and [cyber insurance] providers, while the payoffs of cyber insurance claims received by victims help offset the costs born by victims . . . the costs that InfoSec and [cyber insurance] providers incur in developing and providing their services . . . should be included in the calculus of the total costs of cybercrime.[87]

Direct and Indirect Corporate Costs

Identification of those direct costs to be included in the computation of cyber expense is a task appropriately assigned to the accounting profession for discussion and determination. While some direct costs will be easily identifiable such as: regulatory compliance costs; fines and settlements; ransomware demands paid; lost business attributable to cyber loss—- others will likely best be identifiable with the benefit of audit experience. Professors Wolff and Lehr observe that, "it is much easier to estimate and observe direct costs than indirect costs. However, to estimate total costs, we need to estimate both categories of costs, and because indirect costs may be much larger, this poses a significant enduring challenge for estimates of the total economic impact of cybercrime."[88] Consider:

> Direct costs are those that are directly attributable to a particular cause and may be assigned to an identifiable agent who bears the cost. A firm that suffers a data breach that entails the theft of PII data for its customers may need to suspend its on-line eCommerce operations while it is responding to or recovering from an attack. The lost sales associated with the business interruption may be relatively easy to estimate. Similarly, the expenditures by the victim firm for InfoSec and CyberIns services and products that are used in detection, prevention, and remediation, including for forensic analysis, system repairs or replacement, notifying customers whose [personally identifiable information] [PII] has been breached and providing them with credit monitoring services, and/or in pay-

> ing legal fines or settlements are direct costs that victim firms incur. Losses attributable to fraud perpetrated with the stolen PII are another source of direct cost incurred by the individuals whose PII was breached.
>
> Indirect costs include those that are produced as secondary effects of the incident, or that spillover to others that are not directly involved in the incident. For the victims that are directly involved, the loss of brand reputation or competitive advantage that may adversely impact future sales is a potentially important source of indirect costs from cybercrime. Additionally, the loss of market trust that may slow market growth or increase opportunity costs for all market participants, or the increased likelihood of copycat attacks on other victims are examples of the indirect cost of cybercrime.[89]

Externalities

Professor Tyler Moore has warned that, "The [Information Technology] IT industry is characterized by many different types of externalities where individuals' actions have side effects on others."[90] Professor and seasoned corporate director Trautman recalls a conversation that has been heard in many boardrooms, and it goes like this, "even if we spend every dollar we could borrow . . . We still wouldn't have spent enough on cyber. The North Koreans, Russians, Chinese . . . all these nations are engaged in cyber war. We don't have enough money around here to fight a war . . . That's what governments are for . . ."[91] This pervasive belief results in many boards just pushing the problem off on the government, on others, on their customers and there are few prosecutions, because cyber failures are so pervasive . . . because every corporation has the same problem. Professor Moore states that, "free-riding is likely whenever security depends on the weakest link in the chain: firms do not bother investing in security when they know that other players will not invest, leaving them vulnerable in any case."[92] What externality costs, if any, should be standardized for inclusion by an issuer?

The Impact and Cost of Cyber Crime

Cyber crime takes many forms and continues to evolve in its sophistication. Data breach involving the loss of customer Personal Identifiable Information (PII) remains an expensive proposition for many businesses. During recent years, malware and ransomware has often resulted in substantial expense.[93] The theft of intellectual property remains both discovered and undiscovered by many enterprises. From a public policy standpoint to what extent should intellectual property theft require disclosure and, if disclosable, how measured and should it be amortized, and if so, over what period or time, and by what method?

In their excellent paper to be presented during June 2022,

Professors Anderson, Barton, Böhme, Clayton, Gañán, Grasso, Levi, Moore, and Vasek discuss "Measuring the Changing Cost of Cybercrime."[94] Observing that "Measurement is not straightforward, as cybercrimes frequently cross jurisdictions, and the available statistics are fragmentary,"[95] the authors:

> [F]ollow the European Commission's 2007 Communication "Towards a general policy on the fight against cyber crime", which proposed a threefold definition:
>
> 1. traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems;
>
> 2. the publication of illegal content over electronic media (e.g., child sexual abuse material or incitement to racial hatred);
>
> 3. crimes unique to electronic networks, e.g., attacks against information systems, denial of service and hacking.
>
> To have a yardstick with which to measure changes, we break down fraud figures as follows. We split direct costs from indirect costs, accounting for the costs of security (which often cannot be allocated to specific crime types) and for the social and opportunity costs of reduced trust in online transactions. Where possible we decompose the costs of crime still further, splitting the criminals' revenue from the costs they impose on others (which are often very much larger).
>
> Figure 1 shows our framework, and its cost categories are as follows.
>
> **Criminal revenue** is defined as the gross receipts from crime. It does not include the criminal's 'lawful' business expenses, but we do need to count criminal inputs, so as to get an accurate estimate of the criminal-revenue contribution to GDP. For example, where phishing is advertised by email spam sent by a botnet, we add the criminal revenue of the phisherman (the money withdrawn from victim accounts) and the amount he pays the spammer - possibly split with the 'owner' of the botnet.
>
> **Direct loss** is the value of losses, damage, or other suffering felt by the victims as a consequence of a cybercrime. Examples include money withdrawn from victim accounts; time and effort to reset account credentials after compromise (for both banks and consumers); and lost attention and bandwidth caused by spam messages.
>
> We do not try to measure distress directly; victims are not generally entitled to sue for it and it is hard to measure. Instead we try to estimate the chilling effect that cybercrime - and the fear of cybercrime - have on economic activity. This brings us to:
>
> **Indirect loss** is the value of the losses and opportunity costs imposed on society by the fact that a certain type of cybercrime is carried out. Indirect costs generally cannot be attributed to individual perpetrators or victims. Examples include loss of trust in online banking, leading to reduced revenues from transaction fees and higher costs for maintaining branch staff; sales foregone by online retailers when their fraud engines cause them to decline shopping baskets; reduced uptake by citizens of electronic services whether from companies or governments; cancelled operations due to online

medical services being unavailable; and efforts to clean up machines infected with botnet malware.

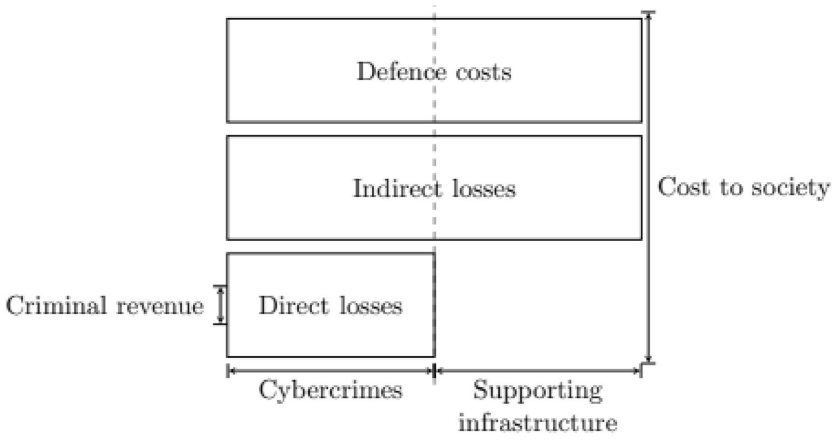
Defence costs measure prevention efforts. They include security products such as spam filters and antivirus; security services provided to individuals, such as awareness raising; security services provided to industry, such as website 'take-down' services; fraud detection and recovery efforts; law enforcement; and opportunity costs such as the inconvenience of missing messages falsely classified as spam.

Like indirect losses, defence costs are largely independent of individual perpetrators and victims - and even of individual types of cybercrime.

In our model, the total social cost of cybercrime is the sum of direct losses, indirect losses, and defence costs. All our figures are in nominal terms. We neglect inflation, as a 2012 dollar is worth $1.11 in 2019 dollars, and the 11% difference is way below our error margin; interest rates have also been near-zero for most of this period. Similarly, differences in exchange rates are insignificant. We are not going to obsessively translate all amounts back and forth between pounds, dollars, and Euros; with the accuracy with which we can work here, these currencies might as well be interchangeable.[96]

Figure 1

Framework for Analysing the Cost of a Cybercrime[97]



Role for Cyber Insurance

For many years corporations and their boards have relied upon insurance to mitigate risk.[98] It is likely that cyber risk insurance carriers have the best information models and experience databases available. Professor Yogesh Malhotra writes, "Quantitative modeling of cyber risk for cyber insurance modeling is at a nascent stage characterized by sparse empirical research and reliable data."[99] Experience indicates the complex nature of this task, and that "the modeler, the decision-maker, the regulator, and, all others involved in developing, testing, managing, or using models need to ensure alignment of the models with the reality. That is simpler said than done given . . . the reality in the context of global cyberspace with increasing interactions is itself dynamically changing."[100]

Data Privacy

Chairman Gensler has recently observed that "customer and client data privacy and personal information" were addressed by Congress in the Gramm-Leach-Bliley Act of 1999 and that, "The Commission adopted Regulation S-P in the wake of that law . . . require[ing] registered broker-dealers, investment companies, and investment advisers to protect customer records and information."[101] Agreement should be reached about what data privacy costs should be included in an enterprise's computation of cybersecurity expense. Should costs related to compliance with the various new state privacy laws be included? For example, under California's CCPA, consumers can request that personal information can be deleted . . . and so on.

IV. RECOMMENDATION

Proposed Working Group Structure

We propose that the SEC establish a "Cybersecurity Disclosure Study Commission" [working title] assigned with the task of obtaining input regarding cyber-cost items that should properly be included in these calculations and disclosures. The Commission may be constructed to provide input from identified stakeholders who are recognized opinion leaders among their various constituencies (suggestions to be provided). Each sub-committee will meet to discuss and formulate their thoughts for subsequent distribution to all Commission members. Stakeholder input from those parties who need detailed knowledge of their actual costs should help mitigate loss resulting from even external "weakest link" cyber exposure vulnerabilities. An initial (but incomplete) list of potential commission members is presented below to foster thought and discussion. Valuable input can be expected from the following stakeholders:

ABA and Securities Bar
Academics and Law Professors
Accounting Profession
AICPA
FASB
PCAOB
CAQ
Business Community
Corporate Directors
NACD leadership
Economists
Governmental Agencies and National Security Interests
[FBI]
Commerce Department [NIST]
Cyber and Infrastructure Security Agency (CISA)-
National Security Community [CIA, DHS, DOD, NSA, OTHERS]
Insurors of Cyber Risk
Securities and Exchange Commission (SEC)
Technology Community
Federal Advisory Act Considerations

We remain indebted to Professor John C. Coffee for bringing our attention to consideration of the 1972 Federal Advisory Committee Act (FACA).[102] Professor Coffee recalls that he experienced this issue several years ago when the Bharara Task Force on Insider Trading was organized—- "and it may be easier not to seek Commission approval or designation (and that body was organized by an SEC Commissioner)."[103] Professor Coffee adds that this problem can be avoided by "having no Commission member or sponsorship."[104]

V. IMPLICATIONS FOR NATIONAL SECURITY

[W]hile [cyber criminals] have become more sophisticated, governments have been sluggish in responding in a meaningful way. As a result, victims are often left to fend for themselves, turning to specialty incident response firms that have developed a niche industry for negotiating decryption. The costs of lost productivity, disrupted operations, inefficiency in markets, and operational recovery likely far outweigh the dollars siphoned out of the world's economies and dumped into illicit activities from human trafficking to the development of weapons of mass destruction. That's right — this malware has afforded Kim Jung Un's ability to continue to expand his nuclear arsenal. How is this still only viewed as a cybercrime?

Christopher C. Krebs
Congressional Testimony
May 5, 2021[105]

During recent years, many examples of nation state sponsored cyber breaches, ransomware, and the use of U.S. domestic social media by foreign interests to create political turmoil through the promulgation of disinformation campaigns are reported.[106] Accordingly, weaknesses in cyber defenses among the business community is a threat to national security interests and vice versa. And, of course, the American population at large will suffer from cyber defense weaknesses elsewhere. SEC Chair Gary Gensler states, "The interconnectedness of our networks, the use of predictive data analytics, and the insatiable desire for data are only accelerating."[107] As observed almost daily, "State actors and non-state hackers alike sometimes try to target various entities and businesses . . . To steal data, intellectual property, or money; lower confidence in our financial system; disrupt economies; or just demonstrate their capabilities. All this puts our financial accounts, savings, and private information at risk."[108] Chairman Gensler continues, "It's not just the economic cost, of course. Cybersecurity is central to national security. The events of the past couple of weeks in Russia and Ukraine have once again highlighted the importance of cybersecurity to our national interest."[109] A recent example of the complex nature of the relationship between nation security interests, cybersecurity, and the business community, is illustrated by Professor Charles Duan's observations that "the national security dimensions of 'races' against technological superpowers such as China, in fields such as artificial intelligence (AI), fifth-generation (5G) mobile communications networks, and quantum computing, has given rise to a national dialogue on spurring domestic innovation, a dialogue into which patents naturally fit."[110]

The Cost of War

Cyber-attacks have now become a cost-effective tool of war. For example, during February 2022, *The Wall Street Journal* reports, "Russia, which has positioned more than 100,000 troops around three sides of Ukraine, is stepping up a destabilization campaign involving cyber-attacks, economic disruption and a new tactic: hundreds of fake bomb threats."[111] The direct costs of war including the financing of troops, transportation, food and supplies—plus lost revenues incurred by any country perceived under threat of invasion due to lost tourist expenditures, lower economic output resulting from uncertainty, and the like. In this case, *The*

Wall Street Journal reports, "Russia is the world's third-largest oil producer, and if a conflict in Ukraine leads to a substantial decrease in the flow of Russian barrels to market, it would be perilous for the tight balance between supply and demand."[112]

Professors Chesney and Citron warn, "Public discourse on questions of policy currently suffers from the circulation of false information.[113] Sometimes lies are intended to undermine the credibility of participants in such debates, and sometimes lies erode the factual foundation that ought to inform policy discourse."[114] Consider:

> Even without prevalent deep fakes, information pathologies abound. But deep fakes will exacerbate matters by raising the stakes for the 'fake news' phenomenon in dramatic fashion (quite literally). Many actors will have sufficient interest to exploit the capacity of deep fakes to skew information and thus manipulate beliefs . . . Others will do it simply as a tactic of intellectual vandalism and fraud . . . In the absence of an agreed reality, efforts to solve national and global problems become enmeshed in needless first-order questions like whether climate change is real. The large-scale erosion of public faith in data and statistics has led us to a point where the simple introduction of empirical evidence can alienate those who have come to view statistics as elitist. (internal citations omitted)[115]

The use of deep fake technologies to achieve a deceptive and malicious altering of reality to deceive observers from the truth may present destructive results in many sectors of life, including sound and fair securities markets and the regulation thereof. Professors Chesney and Citron warn:

> Deep fakes will erode trust in a wide range of both public and private institutions and such trust will become harder to maintain. The list of public institutions for which this will matter runs the gamut, including elected officials, appointed officials, judges, juries, legislators, staffers, and agencies . . . Particularly where strong narratives of distrust already exist, provocative deep fakes will find a primed audience.
>
> Private sector institutions will be just as vulnerable. If an institution has a significant voice or role in society, whether nationally or locally, it is a potential target. More to the point, such institutions already are subject to reputational attacks, but soon will have to face abuse in the form of deep fakes that are harder to debunk and more likely to circulate widely.[116]

A Seat at the Table

Your authors believe that inclusion of informed members of the U.S. national security community is necessary to achieve the best result from this project. All involved in the process of securing domestic cyber infrastructure from nation-state and transnational criminal elements should be represented in this dialogue. The American business community is benefited when any links, and in particular the weakest links, in our mosaic of interconnected data systems is strengthened.

VI. PROPOSED PUBLIC COMPANY CYBERSECURITY OVERSIGHT BOARD

We recommend the Commission should seriously consider asking Congress to pass legislation creating a Public Company Cybersecurity Oversight Board for publicly-traded companies similar to the PCAOB.[117] The PCAOB model is a nonprofit corporation established by Congress to oversee the audits of brokers and dealers registered with the SEC and public companies.[118] Approval of the Board's rules, standards, and budget are governed by the SEC, with the five-member PCAOB Board appointed to staggered five-year terms by the SEC, "after consultation with the Chair of the Board of Governors of the Federal Reserve System and Secretary of the Treasury."[119] In PCAOB's 2021 Annual Report they state "Advancements in technology continue to affect the nature, timing, and preparation of financial information, including preparers' controls around financial information, and the planning and performance of audits."[120] Also during 2021, PCAOB's "Office of the Chief Auditor devoted further attention to [a] research project on data and technology, informed in part by input from a Data and Technology Taskforce, to assess whether there is a need for guidance, changes to PCAOB standards, or other regulatory actions."[121] It now appears to us that the area of cyber threat and risk management requires its own focus and resources.

VII. CONCLUSION

Corporations likely represent the weakest data entry point into U.S. data infrastructure. Capturing structured cost data may allow management, boards, investors, regulators, and national security policy makers to better understand the true costs incurred in cyber defense and breach mediation. Externality costs associated with cyberattack, when ignored by industry, are placing additional burdens upon government and other institutions (such as municipalities, school systems and universities) and citizens when their customer identity data is stolen, resulting in fraud committed against them. Regulators, management, directors, and investors need meaningful and comparable structured data to facilitate decisions about this critically important issue. We believe this proposal is of significant importance and represents a timely contribution in fostering better cooperation between all interested stakeholders in cyber hygiene and security.

APPENDIX

Figure 1

Three channels through which financial accounting information may affect economic performance [observing] Governance role of financial accounting information operates through channel 2[1]

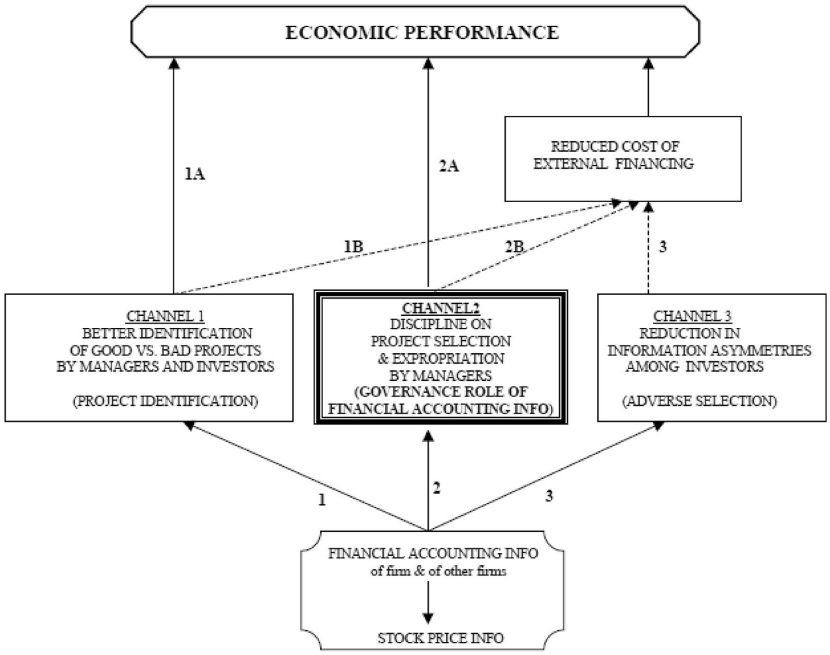
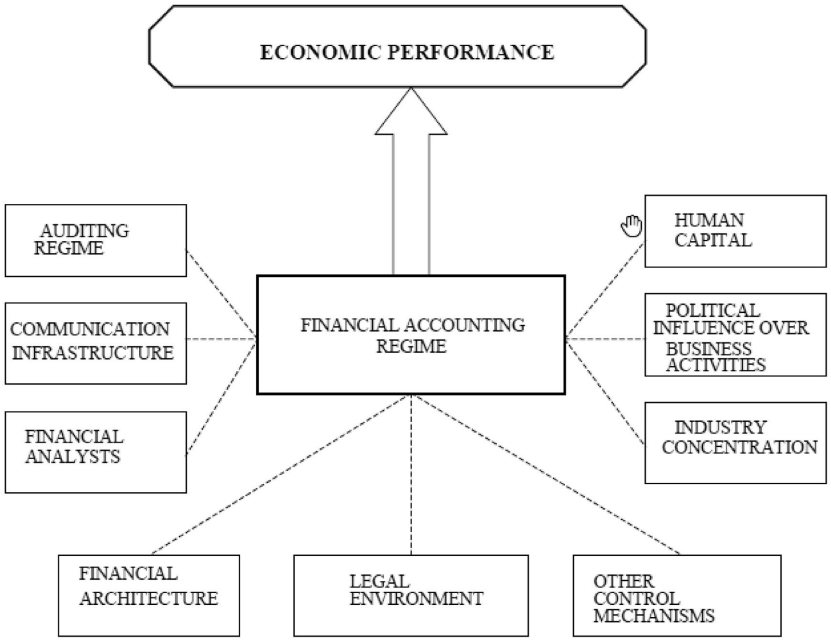


Figure 2

Predicted interactions between financial accounting regimes and other factors in affecting economic performance[2]



NOTES:

[1]Prepared Remarks Before the Principles for Responsible Investment "Climate and Global Financial Markets" Webinar (Jul. 28, 2021), https://www.sec.gov/news/speech/gensler-pri-2021-07-28.

[2]*See* Jack M. Balkin, *The Future of Free Expression in a Digital Age,* 36 PEPP. L. REV. (2008), https://ssrn.com/abstract=1335055; Jack M. Balkin, *Digital Speech and Democratic Culture: a Theory of Freedom of Expression for the Information Society,* 79 N.Y.U. L. REV. (2004), https://ssrn.com/abstract=470842; Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation,* U.C. DAVIS L. REV. (2018), https://ssrn.com/abstract=3038939; Jack M. Balkin, *How to Regulate (and Not Regulate) Social Media,* 1 J. FREE SPEECH L. 71 (2021), https://ssrn.com/abstract=3484114; Jack M. Balkin, *Information Fiduciaries and the First Amendment,* 49 U.C. DAVIS L. REV. (2016), https://ssrn.com/abstract=2675270; Jack M. Balkin, *The Fiduciary Model of Privacy,* 134 HARV. L. REV. FORUM (2020), https://ssrn.com/abstract=3700087.

[3]*See* OXFORD ESSENTIAL QUOTATIONS, OXFORD UNIV. PRESS (4th ed., Susan Ratcliff Eds) (2016), https://www.oxfordreference.com/view/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00006236.

[4]Cybersecurity and Securities Laws, Remarks before the Northwestern

Pritzker School of Law's Annual Securities Regulation Inst., Gary Gensler, Chair, U.S. Securities and Exchange Comm. (Jan. 24, 2022), https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124 (last viewed Feb. 19, 2022).

[5]*See* Lawrence J. Trautman, *Is Cyberattack The Next Pearl Harbor?,* 18 N.C. J. L. & TECH. 232 (2016), http://ssrn.com/abstract=2711059; Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?,* 20 RICH. J.L. & TECH. 13 (2014), http://www.ssrn.com/abstract=2393537; Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?,* 2015 U. ILL. J. L. TECH. & POL'Y 341 (2015), http://ssrn.com/abstract=2548561; Mohammed T. Hussein, Lawrence J. Trautman, Louis Ngamassi & Mason J. Molesky, Climate, Cyber Risk, and the Promise of The Internet of Things (IoT), http://ssrn.com/abstract=3969506.

[6]Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release No. RIN 3235-AM89 (Mar. 9, 2022) [Hereinafter "Proposed Rule"].

[7]Id.

[8]Comments from Professors Lawrence J. Trautman and Neal F. Newman regarding Proposed Rule, *supra* note 6 (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128352-291119.pdf.

[9]*See* Proposed Rule, *supra* note 6 at 55.

[10]*See* Proposed Rule, *supra* note 6 at 55.

[11]Lawrence J. Trautman, Seletha Butler, Frederick Chang, Michele Hooper, Ron McCray & Ruth Simmons, *Corporate Directors: Who They Are, What They Do, Cyber and Other Contemporary Challenges*, 70 BUFFALO L. REV. 459 (2022), http://ssrn.com/abstract=3792382.

[12]*See* Lawrence J. Trautman, Mohammed T. Hussein, Louis Ngamassi & Mason Molesky *Governance of The Internet of Things (IoT)*, 60 JURIMETRICS 315, 332 (Spring 2020), http://ssrn.com/abstract=3443973.

[13]*Id.* at 333.

[14]*See* Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach,* 66 AM. U. L. REV. 1231 (2017), http://ssrn.com/abstract=2883607.

[15]*Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation. Before H. Comm. On Energy & Commerce,* 117th Cong. (2021) (statements and testimony by Mark Zuckerberg, Sundar Pichai, and Jack Dorsey), https://energycommerce.house.gov/committee-activity/hearings/hearing-on-disinformation-nation-social-medias-role-in-promoting.

[16]Tyler Moore, *The economics of cybersecurity: Principles and policy options,* 3 INT'L J. CRITICAL INFRASTRUCTURE PROTECTION, 103, (2010).

[17]*Id.* at 103, 109.

[18]*Id.* at 103.

[19]*See* Proposed Rule, *supra* note 6 at 41.

[20]*See* Proposed Rule, *supra* note 6 at 41.

[21]Prepared Remarks: "Dynamic Regulation for a Dynamic Society" Before the Exchequer Club of Washington, D.C., Gary Gensler, Chair, U.S. Securities and Exchange Comm. (Jan. 19, 2022).

[22]*See* Gensler, *supra* note 3.

[23]*Id.*

[24]*Id.*

[25]Lawrence J. Trautman & Neal Newman, The Environmental, Social and Governance (ESG) Debate Emerges from the Soil of Climate Denial, 53 U. MEM. L. REV. (forthcoming), http://ssrn.com/abstract=3939898.

[26]The Great Depression was the worst economic downturn in the history of the industrialized world, lasting from 1929 to 1939. It began after the stock market crash of October 1929, which sent Wall Street into a panic and wiped-out millions of investors. Over the next several years, consumer spending and investment dropped, causing steep declines in industrial output and employment as failing companies laid off workers. By 1933, when the Great Depression reached its lowest point, some 15 million Americans were unemployed and nearly half the country's banks had failed. https://www.history.com/topics/great-depression/great-depression-history

[27]*See* "A Brief History of the 1930s Securities Laws in the United States - And the Potential Lesson for Today" — Larry Bumgardner, Graziadio School of Business and Management, Pepperdine University — http://www.jgbm.org/page/5%20Larry%20Bumgardner.pdf.

[28]*See* Comparison Between Merit Based Regulation and Disclosure Based Regulation — https://www.mbaknol.com/international-finance/comparison-between-merit-based-regulation-and-disclosure-based-regulation/.

[29]*See* "A Brief History of the 1930s Securities Laws in the United States, *supra* note 27.

[30]LARRY D. SODERQUIST & THERESA A. GABALDON, SECURITIES REGULATION 4 (9th Ed.) (Foundation Press, 2018).

[31]*Id.* at 3.

[32]*Id.* at 4.

[33]*Id.*

[34]*See* Robert A. Prentice, *Enron: A Brief Behavioral Autopsy,* 40 AM. BUS. L.J., 417 (2003); David B. Spence & Robert A. Prentice, *Sarbanes-Oxley as Quack Corporate Governance: How Wise is the Received Wisdom,* 95 GEO. L.J. 1843 (2007); John C. Coffee, Why Do Auditors Fail? What Might Work? What Won't? (January 11, 2019). 597 (2019), European Corporate Governance Institute (ECGI) — Law Working Paper No. 436/2019, https://ssrn.com/abstract=3314338.

[35]*See* Robert A. Prentice, *The Case for Educating Legally Aware Accountants,* 38 AM. BUS. L.J. 597 (2001); John C. Coffee & Hillary A. Sale, *Redesigning the SEC: Does the Treasury Have a Better Idea?*, 95 VA. L. REV. 707 (2009), https://ssrn.com/abstract=1309776.

[36]Claudia Levy, *A.A. Sommer Jr., 77, Dies*, WASH. POST., Jan. 18, 2002, https://www.washingtonpost.com/archive/local/2002/01/18/aa-sommer-jr-77-dies/66b0891d-3eb8-4570-a81d-33d6c1810eac/.

[37]Commissioner Troy A. Paredes, Speech by SEC Commissioner: Twelfth Annual A.A. Sommer, Jr. Lecture on Corporate, Securities and Financial Law (Oct. 27, 2011), *citing* A.A. Sommer, Jr., Therapeutic Disclosure, 4 SEC. REG. L.J. 263, 265 (1976), https://www.sec.gov/news/speech/2011/spch102711tap.htm.

[38]*Id.*, *citing* A.A. Sommer, Jr., *The U.S. Securities and Exchange Commission Disclosure Study*, 1 J. COMP. CORP. L. & SEC. REG. 145, 147 (1978).

[39]*See* Rainer Böhme, & Tyler Moore. The iterated weakest link. 8 IEEE SEC.

& PRIVACY, 53 (2010); Robert Chesney, & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,* 107 CALIF. L. REV. 1753, 1757 (2019); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022); Cesare Fracassi & William J. Magnuson, *Data Autonomy*, 74 VAND. L. REV. (2021), https://ssrn.com/abstract=3545964; Joseph A. Grundfest, Regulation FD in the Age of Facebook and Twitter: Should the SEC Sue Netflix? (January 30, 2013). Rock Center for Corporate Governance at Stanford University Working Paper No. 131, https://ssrn.com/abstract=2209525; Woodrow Hartzog, *What is Privacy? That's the Wrong Question,* 88 U. CHI. L. REV. 1677 (2021), https://ssrn.com/abstract=3970890; Woodrow Hartzog & Neil M. Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020), https://ssrn.com/abstract=3441502; Woodrow Hartzog, *The Public Information Fallacy*, 98 B.U. L. REV. 459 (2019), https://ssrn.com/abstract=3084102; Tal Moran & Tyler Moore, *The phish-market protocol: Secure sharing between competitors,* 8 IEEE SECURITY & PRIVACY, 40 (2010); Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016), https://ssrn.com/abstract=2655719; Scott Shackelford, *Smart Factories, Dumb Policy? Managing Cybersecurity and Data Privacy Risks in the Industrial Internet of Things*, 21 MINN. J. L. SCI. & TECH. 1 (2019); Scott Shackelford, *Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk*, 19 CHAPMAN L. REV. 445 (2016); Daniel J. Solove, *The Myth of the Privacy Paradox,* 89 GEO. WASH. L. REV. 1 (2021), https://ssrn.com/abstract=3536265. Daniel J. Solove, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY. YALE UNIVERSITY PRESS (2011); Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA L. REV. 1252 (2022), https://ssrn.com/abstract=3457563; Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. (Forthcoming 2023), https://ssrn.com/abstract=4024790; Daniel J. Solove & Paul M. Schwartz, An Overview of Privacy Law in 2022, Chapter 1 of PRIVACY LAW FUNDAMENTALS (6th Edition, IAPP 2022), https://ssrn.com/abstract=4072205; Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment*, 90 N.C. L. REV. 1371 (2012); Peter Swire, *Why the U.S. Government Should Have a Privacy Office,* 10 J. TELECOMM. & HIGH TECH. L. 41 (2012); Shauhin A. Talesh & Bryan Cunningham, The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy, Utah Law Review, No. 5, 2021, forthcoming, https://ssrn.com/abstract=3841045; Lawrence J. Trautman, *Rapid Technological Change and U.S. Entrepreneurial Risk in International Markets: Focus on Data Security, Information Privacy, Bribery and Corruption,* 49 CAPITAL U. L. REV. 67 (2021), https://ssrn.com/abstract=2912072; Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327 (2012), https://ssrn.com/abstract=2059154.

[40]Ross Anderson & Tyler Moore. *The economics of information security*, SCIENCE, 610 (2006); Colleen Baker, *When Regulators Collide: Financial Market Stability, Systemic Risk, Clearinghouses and CDS*, 10 VA. L. & BUS. REV. 343 (2016); Orcun Cetin, Mohammad Hanif Jhaveri, Carlos Gañán, Michel van Eeten & Tyler Moore, *Understanding the role of sender reputation in abuse reporting and cleanup,* 2 J. CYBERSECURITY 83 (2016); J. Chen, Henry, E. & Jiang, X., Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach, JOURNAL OF BUSINESS ETHICS (2022); Chesney, Robert, Cybersecurity Law, Policy, and Institutions (version 3.1) (Aug. 2021); Amanda N. Craig, Scott J. Shackelford & Janine S. Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 Am. Bus. L.J., 721 (2015); Benjamin Edwards, Cybersecurity Oversight Liability (May 19, 2019). 35 GA. ST. U. L. REV. 663 (2019), https://ssrn.com/abstract=3390805; Matthew F. Ferraro, *Groundbreaking or Broken? An Analysis of SEC Cyber-Security*

Disclosure Guidance, Its Effectiveness, and Implications, 77 ALBANY LAW REVIEW (2014); Joseph A. Grundfest, The Future of United States Securities Regulation in an Age of Technological Uncertainty (December 2000). Stanford Law and Economics Olin Working Paper No. 210, https://ssrn.com/abstract=253763; Stefan Laube & Rainer Böhme, *The Economics of Mandatory Security Breach Reporting to Authorities*, 2 JOURNAL OF CYBERSECURITY 29 (2016); Thomas M. Lenard, and Rubin, Paul H., An Economic Analysis of Notification Requirements for Data Security Breaches (Jul. 20, 2005), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=765845; Asaf Lubin, *Public Policy and The Insurability of Cyber Risk*, 6 J. L. & TECH. AT TEXAS (forthcoming 2022), https://ssrn.com/abstract=3452833; Jennifer M. Pacella, *The Cybersecurity Threat: Compliance and the Role of Whistleblowers*, 11 BROOKLYN JOURNAL OF CORPORATE, FINANCIAL & COMMERCIAL LAW, (2016), https://ssrn.com/abstract=2803995.

[41]Commissioner Troy A. Paredes, Speech by SEC Commissioner: Twelfth Annual A.A. Sommer, Jr. Lecture on Corporate, Securities and Financial Law (Oct. 27, 2011).

[42]Press Release 2021-42, SEC Announces Enforcement Task Force Focused on Climate and ESG Issues (Mar. 4, 2021), https://www.sec.gov/news/press-release/2021-42 (last viewed July 5, 2021).

[43]Id.

[44]*Id.*

[45]*See* Lawrence J. Trautman, *Bitcoin, Virtual Currencies and the Struggle of Law and Regulation to Keep Pace,* 102 MARQ. L. REV. 447 (2018), https://ssrn.com/abstract=3182867; Neal Newman & Lawrence J. Trautman, *Securities Law: Overview and Contemporary Issues*, 16 OHIO ST. BUS. L.J. 149 (2021), http://ssrn.com/abstract=3790804; Brian Elzweig & Lawrence J. Trautman, When Does A Nonfungible Token (NFT) Become A Security?, __ GA. ST. U. L. REV. (forthcoming), http://ssrn.com/abstract=4055585; Neal Newman & Lawrence J. Trautman, Special Purpose Acquisition Companies (SPACs) and the SEC, 24 U. PA. J. BUS. L. (forthcoming), http://ssrn.com/abstract=3905372; Lawrence J. Trautman, Virtual Art and Non-fungible Tokens, 50 HOFSTRA LAW REVIEW 361 (2022), http://ssrn.com/abstract=3814087; Lawrence J. Trautman & Mason J. Molesky, *A Primer for Blockchain*, 88 UMKC L. REV. 239 (2019), arXiv:1904.03254, https://ssrn.com/abstract=3324660; Lawrence J. Trautman & Alvin C. Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?*, 38 CARDOZO L. REV., 1041 (2017), http://ssrn.com/abstract=2730983; Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?,* 69 CONSUMER FIN. L. Q. REP. 232 (2016), http://ssrn.com/abstract=2786186; Lawrence J. Trautman & George P. Michaely Jr., *The SEC & The Internet: Regulating the Web of Deceit,* 68 CONSUMER FIN. L. Q. REP. 262 (2014), http://www.ssrn.com/abstract=1951148.

[46]Jean Eaglesham & Paul Kiernan, *Climate Disclosures Pose Test for SEC*, WALL ST. J., Feb. 19–20, 2022 at B13.

[47]*Id.*

[48]Lawrence J. Trautman & Neal Newman, The Environmental, Social and Governance (ESG) Debate Emerges from the Soil of Climate Denial, 53 U. MEMP. L. REV. (forthcoming), http://ssrn.com/abstract=3939898.

[49]Press Release 2022-78, SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit, (May 3, 2022), https://www.sec.gov/news/press-release/2022-78.

[50]*Id.*

[51]Mauri L. Osheroff, Mark W. Green & Ruth Armfield Sanders*, Electronic*

Filing and the EDGAR System: A Regulatory Overview (Oct. 3, 2006), https://www.sec.gov/info/edgar/regoverview.htm (last viewed Feb. 19, 2022).

[52]*Id. See also* Release No. 33-6977 (explaining the EDGAR system generally and setting forth rules and procedures that apply to electronic submissions processed by the Division of Corporation Finance and in some cases, to those processed by the Division of Investment Management); Release No. IC-19284 (adopting rules specific to electronic submissions made by investment companies under the Investment Company Act of 1940 and institutional investment managers under Section 13(f) of the Exchange Act); Release No. 35-25746 (adopting rules specific to electronic submissions made by public utility holding companies and their subsidiaries under the Public Utility Holding Company Act of 1935 which was repealed as of early 2006); Release No. 33-6980 (relating to the payment of filing fees, by both paper and electronic filers, to the Commission's lockbox depository at Mellon Bank in Pittsburgh, Pennsylvania, under Rule 3a of the Rules Relating to Informal and Other Procedures).

[53]Osheroff, et al., *supra* note 51.

[54]*Id.*

[55]EDGAR—How Do I, SEC.gov., https://www.sec.gov/edgar/filer-information/how-do-i (last viewed Feb. 19, 2022).

[56]EDGAR Application Programming Interfaces, SEC.gov, https://www.sec.gov/edgar/sec-api-documentation.

[57]*Id.*

[58]*Id.*

[59]*See* Proposed Rule, *supra* note 6 at 49 (internal footnotes omitted).

[60]*See* Gensler, *supra* note 3.

[61]*Id.*

[62]*Id.*

[63]*See* Gensler, *supra* note 3. *See also* Paul Kiernan, *SEC Looks to Boost Cybersecurity Rules,* WALL ST. J., Jan. 25, 2022 at B11.

[64]*See* Proposed Rule, *supra* note 6.

[65]*See* James Rundle, *Cyber Rules test Security chiefs, Boards,* WALL ST. J., Apr. 16–17, 2022 at B3.

[66]*Id.*

[67]*Id.*

[68]Henry T.C. Hu, *Too Complex to Depict? Innovation, "Pure information," and the SEC Disclosure Paradigm,* 90 TEX. L. REV. 1601, 1606 (2012).

[69]*Id.* at 1607.

[70]*Id.* at 1713.

[71]*Id.* at 1714.

[72]*See* Chesney & Citron, *supra* note 39 at 1757 (2019). *See also* Marc J. Blitz, *Deepfakes and Other Non-Testimonial Falsehoods:When is Belief Manipulation (not) First Amendment Speech?,* 23 YALE J. L. & TECH. 160 (2020); Donald C. Langevoort, Technological Evolution and the Devolution of Corporate Financial Reporting (2003), https://ssrn.com/abstract=480704.

[73]Jeffery Atik & Valentin Jeutner *Quantum computing and computational law*, L. INNOVATION & TECH., (2021), https://ssrn.com/abstract=3490930; Jeffery

Atik, Quantum Computing and the Legal Imagination, 18 SCITECH LAWYER 12 (2022), https://ssrn.com/abstract=4087044; Luigi Bruno & Isabella Spano, *Post-Quantum Encryption and Privacy Regulation: Can the Law Keep Pace with Technology?*, EUR. J. PRIVACY L. & TECH. (2021), https://ssrn.com/abstract=3920272; CHRIS JAY HOOFNAGLE & SIMSON GARFINKEL, LAW AND POLICY FOR THE QUANTUM AGE CAMBRIDGE UNIVERSITY PRESS (2022), https://ssrn.com/abstract=4007638; Valentin Jeutner, *The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers,* 1 MORALS & MACHINES 52 (2021) https://ssrn.com/abstract=3820003; Mauritz Kop, *Establishing a Legal-Ethical Framework for Quantum Technology,* YALE JOURNAL OF LAW & TECHNOLOGY (YJoLT), The Record, March 30 2021, https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology, https://ssrn.com/abstract=3814422; Mauritz Kop, *Quantum Computing and Intellectual Property Law,* 35 BERKELEY TECH. L.J. 8 (2021), https://btlj.org/2022/02/quantum-computing-and-intellectual-property-law/; Lindsay Rand & Theodore Rand, The 'Prime Factors' of Quantum Cryptography Regulation (2021), https://ssrn.com/abstract=3904342; Andre van Tonder, A Lambda Calculus for Quantum Computation, Science Direct Working Paper No S1574-034X(04)70285-9 (2003), https://ssrn.com/abstract=2978398; Yazhen Wang & Hongzhi Liu, *Quantum Computing in a Statistical Context,* 9 ANNUAL REVIEW OF STATISTICS AND ITS APPLICATION, 479 (2022), https://ssrn.com/abstract=4065375; Vyacheslav I. Yukalov & Didier Sornette, *Scheme of Thinking Quantum Systems,* 6 LASER PHYSICS LETTERS, 833 (2009), https://ssrn.com/abstract=1470624.

[74]Robert M. Bushman & Abbie J. Smith, *Financial Accounting Information and Corporate Governance,* 32 J. ACCT. & ECON. 1 (2001).

[75]*Id.*

[76]William J. Magnuson, *A Unified Theory of Data*, 58 HARV. J. ON LEGIS. 23 (2021).

[77]*See* H. Justin Pace & Lawrence J. Trautman, Mission Critical: *Caremark. Blue Bell,* and Director Responsibility for Cybersecurity Governance, ___ WISC. L. REV. (forthcoming), http://ssrn.com/abstract=3938128; Lawrence J. Trautman, *Managing Cyberthreat,* 33 SANTA CLARA HIGH TECH. L.J. 230 (2016), http://ssrn.com/abstract=2534119; Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 29 JOHN MARSHALL J. COMP. & INFO. L. 313 (2011), http://www.ssrn.com/abstract=1947283; Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis,* 20 PITT. J. TECH. L. & POL'Y 41 (2020), http://ssrn.com/abstract=3363002; Lawrence J. Trautman, *How Google Perceives Customer Privacy, Cyber, E-Commerce, Political and Regulatory Compliance Risks,* 10 WM. & MARY BUS. L. REV. 1 (2018), https://ssrn.com/abstract=3067298; Lawrence J. Trautman, *E-Commerce, Cyber and Electronic Payment System Risks: Lessons from PayPal,* 17 U.C. DAVIS BUS. L.J. 261 (Spring 2016), http://www.ssrn.com/abstract=2314119; Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?,* 11 DEPAUL BUS. & COMM. L.J. 205 (2013), http://www.ssrn.com/abstract=2137747; Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment,* 11 FLA. ST. U. BUS. REV. 75 (2012), http://www.ssrn.com/abstract=1998489; Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance,* 13 HASTINGS BUS. L.J. 275 (2017), http://ssrn.com/abstract=2623219.

[78]*See SEC Corporate Finance Disclosure Guidance: Topic No. 2: Cybersecurity*, DIV. OF CORP. FIN., SEC (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[79]Lawrence A. Hamermesh, *Calling Off the* Lynch *Mob: The Corporate Director's Fiduciary Disclosure Duty*, 49 VAND. L. REV. 1087, 1097 (1996).

[80]*Id.* at 1091.

[81]Advancing Cyber Resilience: Principles and Tools for Boards, WORLD ECONOMIC FORUM (Jan. 2017).

[82]*Id.*

[83]Trautman, et al., *supra* note 11.

[84]Robert M. Bushman & Abbie J. Smith, *Financial Accounting Information and Corporate Governance,* 32 J. ACCT. & ECON. 1, 113 (2001).

[85]*Id.* at 114.

[86]Josephine Wolff & William Lehr, *Degrees of Ignorance about the Costs of Data Breaches: What Policymakers Can and Can't Do about the Lack of Good Empirical Data,* 16 (2017), https://ssrn.com/abstract=2943867.

[87]*Id.*

[88]*Id.*

[89]*Id.*

[90]Moore, *supra* note 16.

[91]*See* Trautman, et al., *supra* note 11.

[92]Tyler Moore, *supra* note 16, *citing H. Varian, System Reliability and Free Riding, in* 12 ECON. INFO. SEC. L.J. CAMP, S. LEWIS (Eds) Kluwer Acad. Pub. (2004).

[93]*See* David D. Schein & Lawrence J. Trautman, *The Dark Web and Employer Liability,* 18 COLO. TECH. L.J. 49 (2020), http://ssrn.com/abstract=3251479; Lawrence J. Trautman, Mohammed T. Hussein, Emmanuel U. Opara, Mason J. Molesky & Shahedur Rahman, *Posted: No Phishing*, 8 EMORY CORP. GOV. & ACCT. REV. 39 (2021), http://ssrn.com/abstract=3549992; Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761 (2018), http://ssrn.com/abstract=2982629; Lawrence J. Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503 (2019), http://ssrn.com/abstract=3238293.

[94]Ross Anderson, Chris Barton, Ranier Böhme, Clayton, Gañán, Grasso, Levi, Moore, and Vasek, Measuring the Changing Cost of Cybercrime (unpub. ms.), https://www.lightbluetouchpaper.org/2019/05/30/the-changing-cost-of-cybercrime/.

[95]*Id.* at 2.

[96]*Id.* at 3.

[97]*Id.*

[98]*See* Lawrence J. Trautman & Kara Altenbaumer-Price, *D&O Insurance: A Primer*, 1 AM. U. BUS. L. REV. 337 (2012), http://www.ssrn.com/abstract=1998080.

[99]Yogesh Malhotra, Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models Using Quantitative Finance and Advanced Analytics, iv (Jan. 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553547.

[100]*Id.* at 158; *See also* Tom Baker & Sean J. Griffith, *Predicting Corporate Governance Risk: Evidence from the Directors' and Officers' Liability Insurance Market,* 74 CHICAGO L. REV. 487, (2007), https://ssrn.com/abstract=909346; Tom Baker & Griffith, Sean J., The Missing Monitor in Corporate Governance: The Directors' & Officers' Liability Insurer. 95 GEO. L.J., 1795, (2007), https://ssrn.co

m/abstract=946309; Tom Baker & Sean J. Griffith, *How the Merits Matter: D&O Insurance and Securities Settlements,* 157 U. PA. L. REV. 755, (2009), https://ssrn.com/abstract=1101068; Tom Baker, Back to the Future of Cyber Insurance. PLUS Journal 1 (2019), U of Penn, Inst for Law & Econ Research Paper No. 20-40, https://ssrn.com/abstract=3625770; H. Bryan Cunningham, & Shauhin A. Talesh, *Uncle Sam Re: Improving Cyber Hygiene and Increasing Confidence in the Cyber Insurance Ecosystem Via Government Backstopping,* 28 CONN. INS. L.J. 1 (2021); Jay Kesan, & Linfeng Zhang, *When is a Cyber Incident Likely to be Litigated and How Much Will It Cost? An Empirical Study*, 28 CONN. INS. L.J. 123 (2021); Kyle D. Logue, & Adam B. Shniderman, *The Case for Banning (and Mandating) Ransomware Insurance*, U of Michigan L. & Econ Research Paper No. 21-040, (August 18, 2021), https://ssrn.com/abstract=3907373.

[101]*See* Gensler, *supra* note 3. *See also* Wayne Unger, *How the Poor Data Privacy Regime Contributes to Misinformation Spread and Democratic Erosion,* 22 COLUM. SCI. & TECH. L. REV. 308 (2021), https://ssrn.com/abstract=3762609; Wayne Unger, *Reclaiming Our Right to Privacy by Holding Tech. Companies Accountable*, 27 RICH. J. L. & TECH. 1 (2020), https://ssrn.com/abstract=3722672.

[102]Pub L. 92-463, Oct. 6, 1972, 86 STAT. 770.

[103]Email from John C. Coffee to Lawrence J. Trautman dated 4-25-2022.

[104]Email from John C. Coffee to Lawrence J. Trautman dated 5-2-2022.

[105]Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis: Hearings Before the H. Comm. On Homeland Security, Subcomm. On Cybersecurity, Infrastructure Protection, & Innovation, 117th Cong. (2021) (Statement by Christopher C. Krebs, Fmr. Dir. Of the Cybersecurity and Infrastructure Security Agency (CISA)).

[106]Jonathan Zittrain, Engineering an Election. 127 HARV. L. REV. FORUM, 335, (2014), https://ssrn.com/abstract=2457502.

[107]*See* Gensler, *supra* note 3.

[108]*Id.*

[109]*Id. See also* David Uberti & Dustin Volz, *Destructive Malware Hit Hours Before Military Offensive,* WALL ST. J., Feb. 25, 2022 at A8; Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who & How It Works,* 5 J. L. & CYBER WARFARE 147 (2016), http://ssrn.com/abstract=2638448; Lawrence J. Trautman, *Impeachment, Donald Trump and The Attempted Extortion of Ukraine*, 40 PACE L. REV. 141 (2020), http://ssrn.com/abstract=3518082.

[110]Charles Duan, *Of Monopolies and Monocultures: The Intersection of Patents and National Security*, 36 SANTA CLARA HIGH TECH. L.J. 369 (2020), https://ssrn.com/abstract=3820782. *See also* Janine S. Hiller & Roberta S. Russell, *The Challenge and Imperative of Private Sector Cybersecurity: An International Comparison*, 29 COMPUTER L. & SEC. REV. 236 (2013).

[111]James Marson, *Hybrid War Already Started, Kyiv Says,* WALL ST. J., Feb. 14, 2022 at A1.

[112]Christopher M. Matthews & Collin Eaton, *Ukraine Threat Pushes Oil Near $100,* WALL ST. J., Feb. 14, 2022 at A1.

[113]*See* Chesney & Citron, *supra* note 39 at 1777, *citing* Steve Lohr, *It's True: False News Spreads Faster and Wider. And Humans Are to Blame,* N.Y. TIMES, (Mar. 8, 2018).

[114]Chesney & Citron, *supra* note 39 at 1777.

[115]*Id.*

[116]*Id.* at 1779. *See also* Jessica M. Silbey & Woodrow Hartzog, *The Upside of Deep Fakes,* 78 MD. L. REV. 960 (2019), https://ssrn.com/abstract=3452633.

[117]We remain indebted to Arthur E. Wilmarth, Jr., Professor Emeritus of Law at the George Washington University Law School for this thoughtful, helpful and wonderful suggestion.

[118]Public Company Accounting Oversight Board, 2021 Annual Report at 3., https://pcaobus.org/about/annual-report.

[119]*Id.*

[120]*Id.* at 9.

[121]*Id.*

[1]Bushman & Smith, *supra* note 74 at 113.

[2]Bushman & Smith, *supra* note 74 at 114.