CYBERSECURITY: SHOULD THE SEC BE STICKING ITS NOSE UNDER THIS TENT?

Loren F. Selznick and Carolyn LaMacchia†

TABLE OF CONTENTS

I. Introduction 35
II. Cybersecurity Breaches 37
A. Effects on Stock Price 41
B. How the SEC Has Addressed Cybersecurity 42
1. The SEC's Job 42
2. SEC Response to Cybersecurity Risks 45
a. 2011 Cybersecurity Disclosure Guidance 45
b. Cybersecurity Examinations 51
c. Weaknesses in the SEC Response 52
d. The Guidance Has Been Ineffective 53
e. Problems with the Cybersecurity Examinations 56
C. What the SEC Should Be Doing 61
III. Conclusion 69

I. INTRODUCTION

On January 29, 2015, Anthem, Inc. learned of a cyberattack that occurred over the course of several weeks.[1] Anthem, the country's second-largest health insurer, reported unauthorized access to a database containing 80 million customer and employee records.[2] Critical information accessed included Social Security numbers, birthdays, street and email addresses, and income data.[3] Working closely with the Federal Bureau of Investigation, the company has taken corrective measures, but the attackers have not been identified.[4] According to media reports, Anthem will soon deplete its $100 million cyber-

† Dr. Selznick (J.D. Cornell University) is an Assistant Professor of Business Law at Bloomsburg University of Pennsylvania and Dr. LaMacchia (Ph.D. Nova Southeastern University) is an Assistant Professor of Information and Technology Management, also at Bloomsburg University of Pennsylvania.

1. *How to Access & Sign Up for Identity Theft Repair & Credit Monitoring Services*, ANTHEM FACTS, https://www.anthemfacts.com (last visited Mar. 6, 2016).
2. *Id.*
3. *Id.*
4. *Id.*

insurance coverage just to notify the victims and provide free identity-theft protection and credit monitoring in the wake of this breach.[5] Anthem's predicament is commonplace—managing a loss that is not readily apparent, unpredictable, and costly. With more business operations dependent upon technology, cybersecurity breaches occur on a daily basis and impact entities of all sizes.

Investors envision similar cybersecurity breaches at their own companies. What if hackers obtained the debit and credit card information of retail customers? What if the cloud storage the company maintained for clients were breached? What if medical information were left unprotected? What if trade secrets were revealed? For businesses, investors need information to evaluate the likelihood of a cybersecurity breach and its potential effect on overall company health.

Similarly, cybersecurity breaches could affect the operation of the securities markets themselves. What if a broker-dealer network were breached? Would investor funds and identity information be protected? Could hackers manipulate stock prices, post phantom transactions, or shut down exchanges?

Enter the Securities and Exchange Commission (SEC), whose role is to protect investors by requiring companies to disclose material risks to the bottom line and by addressing risks to overall market function.[6] Serious cybersecurity breaches have the potential to affect the stability and even viability of publicly-traded companies, traders, and exchanges. The SEC has, therefore, considered this emerging risk a priority. On the one hand, the SEC wants sufficient disclosure to ensure that investors are not blindsided by a major cybersecurity breach. On the other hand, required disclosures or remedial steps should not make such a breach more likely.

The SEC has issued a guidance statement for disclosures about cybersecurity risks to publicly-traded companies.[7] It has also required individual companies to provide additional information about cybersecurity risks.[8] The SEC response appears to have been both too much and too little at once. The agency has companies disclosing the kinds of minor cybersecurity breaches that everyone experiences, which are annoying, but not life-threatening.[9] Listing them camouflages the major risks that concern investors. When a major breach occurs, however, the disclosures required are ineffective.

The SEC has also conducted cybersecurity examinations of broker-dealers and transfer agents. Pursuant to these examinations, it collected information about the approaches reporting companies use to protect

5. Mary A. Chaput, *Calculating the Colossal Cost of a Data Breach*, CFO (Mar. 24, 2015), http://ww2.cfo.com/data-security/2015/03/calculating-colossal-cost-data-breach/.

6. *About the SEC*, SEC, http://www.sec.gov/about/whatwedo.shtml (last visited Feb. 29, 2016).

7. SEC, DIV. OF CORP. FIN., CF DISCLOSURE GUIDANCE: TOPIC NO. 2, CYBERSECURITY (Oct. 13, 2011) [hereinafter TOPIC NO. 2], http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

8. SEC, OFF. OF COMPLIANCE INSPECTIONS & EXAMINATIONS, NAT'L EXAMINATION PROGRAM, RISK ALERT: OCIE CYBERSECURITY INITIATIVE (Apr. 15, 2014) [hereinafter RISK ALERT], https://www.sec.gov/ocie/announcement/ Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.

9. TOPIC NO. 2, *supra* note 7.

themselves against security breaches. The agency then studied the efforts of the industry as a whole.[10] Recent criticism of the cybersecurity measures at the SEC itself, however, brings into question whether collecting the sensitive information actually increases the risk to investors.[11] The SEC required regulated entities to hand over information that may have been too sensitive in light of its own cybersecurity weaknesses.

This article, an interdisciplinary study, examines first, cybersecurity risks to the investing public, second, whether the SEC is the appropriate agency to address these risks, third, what the SEC is doing about them and the flaws in its response, and, fourth, whether its response can be improved.

II. CYBERSECURITY BREACHES

Cybersecurity breaches come in many forms and are used to steal data assets, disrupt company operations, extort information, or damage reputations.[12] The hacking of corporations is rampant in the United States, prompting law enforcement to observe that there are two kinds of companies: those who have been hacked, and those who do not know they have been hacked.[13] In some cases, companies are not aware for an extended period that a breach is occurring. In January, the New York Times revealed that its computers were compromised by Chinese hackers for four months.[14] The problem is considered critical and its extent is much worse than has been reported. Companies generally do not disclose a breach unless required by law; many breaches, particularly those in small and mid-sized businesses go unreported.[15]

Data, including customer contact information, credit card data, health data, and valuable intellectual property, is most often the target of a breach. Surveys reveal the continued rise of the lucrative black market in credit card data, health credentials, and personal identifying information.[16] In late 2013,

10. RISK ALERT, *supra* note 8.

11. *U.S. SEC's Information Technology at Risk of Hacking—Report*, REUTERS (Apr. 17, 2014, 4:21 PM), http://www.reuters.com/article/sec-cybercrime-security-idUSL2N0N91GU20140417.

12. *See, e.g.*, Michael J. Lebowitz, *The Cyberenemy: Using the Military Justice System to Prosecute Organized Computer Attackers*, 2013 U. Ill. J.L. TECH. & POL'Y 83, 86–87 (2013) (discussing how to prosecute cyberattacks and organized groups using the military justice system).

13. James Cook, *FBI Director: China Has Hacked Every Big US Company*, BUS. INSIDER (Oct. 6, 2014), http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10 (quoting FBI Director James Comey as having said on the CBS program *60 Minutes*, "[t]here are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese.").

14. Nicole Perlroth, *Hackers in China Attacked the Times for the Last 4 Months*, N.Y. TIMES (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html. Experts believe the hackers were attempting to identify the sources for an article describing how Chinese Prime Minister Wen Jiabo accumulated a billion dollar fortune through questionable business dealings. Geoffrey Ingersoll & Michael B. Kelley, *A Digital Trail of Evidence Linked the NYT Hack to China*, BUS. INSIDER (Feb. 1, 2013), http://www.businessinsider.com/nyt-china-hack-how-we-know-203-2.

15. Fred Donovan, *Many Major Financial Data Breaches Go Unreported, Say IT Pros*, FIERCEITSECURITY (July 2, 2015), http://www.fierceitsecurity.com/story/many-major-financial-data-breaches-go-unreported-say-it-pros/2015-07-02.

16. Sophie Curtis, *Cyber Black Market 'More Profitable than Drug Trade*; TELEGRAPH (Mar. 26, 2014), http://www.telegraph.co.uk/technology/internet-security/10724704/Cyber-black-market-more-

several data aggregator companies, including Dun & Bradstreet, LexisNexis, and Kroll Background American, were hacked by the introduction of botnet software on compromised servers.[17] Botnets are mechanized collection tools that can target organizations of any size for consumer and business data.[18] Attackers worked undetected for months to siphon massive amounts of personal identifying information.[19] Unlike credit card numbers, which can be cancelled, employment details, addresses, and social security numbers can be used repeatedly in a widening circle of fraud. The impact of this type of data theft can be long term as cyber criminals sell personal identifying information on the black market.

"Some of the largest attacks in the past year or so included eBay (145 million users), Home Depot (109 million customers), JPMorgan Chase (83 million customers), Target (70 million customers), and Michaels Stores (3 million customers)."[20] The attractiveness of most information is independent of the size of the organization, however, because automated techniques access multiple targets. Although not usually publicized, small and mid-sized businesses have been the target of about sixty percent of data-driven breaches.[21] These organizations are attractive to cyber thieves for a number of reasons. Smaller businesses typically have neither the in-house expertise nor the budget to implement sophisticated cybersecurity prevention measures.[22] In addition, many mistakenly believe cyber thieves prefer larger targets.[23] It is the data and the vulnerability of the organization, not its size, that make a company the target of a cybersecurity breach.

Cybercrime can also target securities market operations. Stock prices tend to increase during periods with a large volume of trading activity.[24] Criminals have taken advantage of this phenomenon using a variety of deceitful techniques. An example is the "pump-and-dump" scheme where promoters claim to have "inside" information about an impending development that will have a positive impact on the price of stock.[25] The promoters sell their own shares after the stock price is "pumped" up by the buying frenzy they

profitable-than-drug-trade.html.

17. Brian Krebs, *Data Broker Giants Hacked by ID Theft Service*. KREBSONSECURITY.COM (Sept. 13, 2013), http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/.

18. *Botnets 101: What They Are and How to Avoid Them*, FBI (July 5, 2013), https://www.fbi.gov/news/news_blog/botnets-101/botnets-101-what-they-are-and-how-to-avoid-them.

19. Krebs, *supra* note 17.

20. William Atkinson, *Cybersecurity Challenges for Small Business*, BENEFITSPRO (Feb. 9, 2015), http://www.benefitspro.com/2015/02/09/cybersecurity-challenges-for-small-business.

21. Jay Jacobs, *Analyzing Ponemon Cost of Data Breach*, DATADRIVENSECURITY (Dec. 11, 2014), http://datadrivensecurity.info/blog/posts/2014/Dec/ponemon/.

22. Taylor Armerding, *Why Criminals Pick on Small Business*, CSO (Jan. 12, 2015), http://www.csoonline.com/article/2866911/cyber-attacks-espionage/why-criminals-pick-on-small-business.html#comments.

23. Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUS. (Mar. 13, 2014), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

24. Ekkehert Boehmer & Juan Wu, *Short Selling and the Price Discovery Process*, 26 REV. FIN. STUD. 2, 287–322 (2013).

25. *"Pump-and-Dumps" and Market Manipulations*, SEC [hereinafter PUMP AND DUMP], https://www.sec.gov/answers/ pumpdump.htm (last visited Feb. 29, 2016).

created.[26] After the selling hype and after the fraudsters "dump" (sell) their shares, the price typically falls, and investors lose their money.[27] A variation of the scheme is the "hack, pump, and dump" which incorporates a cybersecurity breach to steal a company repository of customers' personal identifying information.[28] Stolen account information is used to generate a large volume of stock purchases which artificially manipulate stock prices.[29] As in the "pump-and-dump" technique, the criminal operation sells its shares when the price is high.[30] The stock's price plummets, leaving investors defrauded with "significant losses."[31] "Pump-and-dump" activity violates the Security Exchange Rule 10b-5.[32]

Hackers operate in a variety of ways. Technological similarity from company to company makes their work easier. Most companies, regardless of size, are operating with a technology-driven business model.[33] The typical technology infrastructure consists of a common set of software components including operating, network, and database management systems.[34] In the global commercial marketplace, there are relatively few vendors offering these systems when compared with applications.[35]

In addition, designs of these systems are based on quality standards that have evolved for the efficient and secure processing of data and the interoperability of components. Appropriately implementing secured coding standards adds additional, often significant, cost in areas including software developer training and product verification.[36] Unfortunately, mass-market software sales are not governed by appropriate product-risk norms; as a result, market conditions exist in which sellers profit by offering vulnerability-ridden software.[37] The prevailing consensus is that software programs are sold with an unacceptable number of security vulnerabilities that are gradually fixed

---

26. *Id.*

27. *Id.*

28. *See, e.g.*, Michael Riley & Jordan Robertson, *Digital Misfits Link JPMorgan Hack to Pump-and-Dump Fraud*, BLOOMBERG BUS. (July 22, 2015), http://www.bloomberg.com/news/articles/2015-07-21/fbi-israel-make-securities-fraud-arrests-tied-to-jpmorgan-hack (describing the hack-pump-and-dump scheme against JP Morgan).

29. *Id.*

30. PUMP AND DUMP, *supra* note 25.

31. Brandon Stosh, *Three Men Arrested in Biggest Bank Hacking Scheme Breaching JP Morgan Among Others*, FREEDOM HACKER (Nov. 11, 2015), https://freedomhacker.net/three-men-arrested-biggest-bank-hacking-scheme-breaching-jp-morgan-4741/.

32. 17 C.F.R. § 240.10b-5 (2014).

33. HARV. BUS. REV. ANALYTIC SERVICES, THE REINVENTION OF BUSINESS: NEW OPERATING MODELS FOR THE NEXT-GENERATION ENTERPRISE (2012), https://hbr.org/resources/pdfs/tools/17360_HBR_Cognizant_Report_webview.pdf.

34. DAVID A. PATTERSON & JOHN L. HENNESSY, COMPUTER ORGANIZATION AND DESIGN: THE HARDWARE/SOFTWARE INTERFACE (5th ed. 2013).

35. DANIEL P. SIEWIOREK & ROBERT S. SWARZ, RELIABLE COMPUTER SYSTEMS: DESIGN AND EVALUATION (3rd ed. 1998).

36. Ronny Grey & Andrea Fried, *"Standard Bibles" and Mediators As a Way of Software Development Organizations to Cope with the Multiplicity and Plurality of Standards*, 12 INT'L J. IT STANDARDS & STANDARDIZATION RES. 57 (2014).

37. Richard Warner & Robert H. Sloan, *Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access*, 2012 U. ILL. J.L. TECH. & POL'Y 45 (2012).

through the release of software patches.[38] It is the responsibility of the software user to update the software version with a software patch in order to remove the vulnerability from the user's system.[39] The strengths and weaknesses of these consistently designed systems are well known to both technology professionals and the cybercriminal world. After the release of a software patch, cybercriminals can continue to take advantage of a software vulnerability on systems which the patch has not been installed.

This year, the University of California, Berkley, was hit with a data breach that exposed students' Social Security numbers and families' financial information.[40] Hackers accessed the information through a known vulnerability on an unpatched researcher's computer.[41] It is not surprising that reports of security breaches reveal that most attacks resulted not from clever attackers discovering new kinds of flaws, but rather from repeated tries of well-known exploits.[42]

As cyber-attacks on retail, technology, and industrial companies increase so does the importance of cybersecurity. From brute-force attacks on networks[43] "to malware compromising credit card information to disgruntled employees sabotaging networks from the inside, companies and their customers need to secure their data."[44] An organization's technical security architecture includes firewalls, hardened hosts,[45] intrusion detection systems, and other tools to form a complete system of protection. Without a technical security architecture, companies will be unable to create a comprehensive wall against attackers. Technical security architecture often includes defense-in-depth, which requires multiple countermeasures to be defeated for an attack to succeed.[46] This is important because every security measure has vulnerabilities.

It is never possible to eliminate risks and completely insulate information. It is technically impossible to protect against all future events. Even if it were technically possible to protect against all risk, comprehensive security protections would be prohibitively expensive and impede business operations. High-security environments tend to be inefficient.[47] Security is never free and

38. STEVE MAGUIRE, WRITING SOLID CODE (2013).

39. Janet Gilmore, *Campus Announces Data Breach*, BERKELEY NEWS (Apr. 30, 2015), http://news.berkeley.edu/2015/04/30/campus-announces-data-breach/.

40. *Id.*

41. *Id.* The vendors of the software components issue software fixes, "patches," to their customers in response to recommendations in internal quality control review reports and to cybersecurity breaches. It is the customer's responsibility to install the software patch to remove the vulnerability.

42. GEORGE CYBENKO ET AL., ADVERSARIAL AND UNCERTAIN REASONING FOR ADAPTIVE CYBER DEFENSE: BUILDING THE SCIENTIFIC FOUNDATION. INFORMATION SYSTEMS SECURITY 1–8 (2014).

43. A brute-force attack is a systematic attempt, usually through a simple computer program, of all possible keys or passwords until the correct one is found.

44. Riley Walters, *Cyber Attacks on U.S. Companies in 2014*, HERITAGE, http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014 (last visited Feb. 29, 2016).

45. Any device (servers, routers, computers, tablets, etc.) connected to a network is a host. Each device requires cybersecurity protection to become a "hardened host."

46. *Datasäkerhet och integritet*, DALARNA UNIV., http://users.du.se/~hjo/cs/ik1080/presentations/som_pdf/ch2.pdf.

47. *Boyle Applied Security Chapter 2 Flashcards*, QUIZLET (Feb. 17, 2016, 5:48 PM), https://quizlet.com/76382653/boyle-applied-security-chapter-2-flash-cards/.

seldom inexpensive with costs including not only the initial cost of the security device but the labor to implement, operate, and maintain. "The wave of recent data breaches at big-name companies such as JPMorgan Chase, Home Depot, and Target raises questions about the effectiveness of the private sector's information security."[48]

A. Effects on Stock Price

Industry analysis has shown that the stock price of an organization is not adversely impacted by the news of a data breach.[49] When an official announcement of a cybersecurity breach is made, stockholders react indifferently. What explains this phenomenon? Recovering from a cybersecurity breach is typically very expensive; why isn't the announcement of a breach reflected in the price of stock? Several factors may explain this.

It is difficult to quantify the cost and recovery timeline associated with a cyberattack on a business. While the short-term stock price is unaffected in the wake of a cybersecurity breach, companies face long-term consequences, including spending millions of dollars to upgrade security systems and to settle lawsuits. Once the extent of the breach is determined, stock prices react as they do to other triggers that adversely impact the long-term earning potential of the corporation.[50]

Determining the cost of a cybersecurity breach is a difficult task and should include both direct and indirect expenses incurred by the organization.[51] "Direct expenses include legal fees, regulatory fines, call centers, and credit monitoring subscription fees."[52] Once a breach is discovered, the full value of direct expenses is difficult to estimate because of the extended timeframe for discovering all parties impacted by the breach.[53] "It is even more difficult to calculate indirect costs, such as the loss of revenue and the expenses from the negative impact on the reputation, brand, and marketplace image."[54] "The average cost of cybercrime incidents rises significantly each year for U.S. organizations with an annual average in 2014 of $8.6 million for a retail company."[55] "It is even higher in other sectors; the annual average cost per company of successful cyber-attacks increased to $20.8 million in financial services, $14.5 million in the technology sector, and $12.7 million in communications industries."[56] "Post-breach share-price declines have only

48. Walters, *supra* note 44.

49. Elena Kyochko & Rajiv Pant, *Why Data Breaches Don't Hurt Stock Prices*, HARV. BUS. REV. (Mar. 31, 2015), https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

50. *Id.*

51. Mary A. Chaput, *Calculating the Colossal Cost of a Data Breach*, CFO (Mar. 24, 2015), http://ww2.cfo.com/data-security/2015/03/calculating-colossal-cost-data-breach/.

52. *Breach Costs*, CYBER RISK HUB, http://www.cyberriskhub.com/breach-costs/ (last visited Feb. 29, 2016).

53. Kristin Shields, *Cybersecurity: Recognizing the Risk and Protecting Against Attacks*, 19 N.C. BANKING INST. J. 345 (2015).

54. *Breach Costs*, *supra* note 52.

55. Walters, *supra* note 44.

56. Michael A. Robinson, *Get in on the "Ground Floor" of this National Security Investment*, STRATEGIC TECH INVESTOR (Sept. 9, 2015), http://strategictechinvestor.com/2015/09/get-in-on-the-ground-

had lasting effect following company disclosures of clear, direct and immediate impact on business operations, such as warnings that high costs would hurt profitability."[57]

B. How the SEC Has Addressed Cybersecurity

Given the risk of substantial losses, the SEC has taken up the cybersecurity issue. This is consistent with its mission to protect the investing public by requiring disclosure of material information.[58] Whether the information it has thus far demanded on cybersecurity is actually "material" and whether the SEC is equipped to handle the sensitive cybersecurity information it is gathering in its examinations, however, is questionable.

1. The SEC's Job

The SEC has a "public policy mission of protecting investors and safeguarding the integrity of the markets."[59] This has been further refined by the agency itself as a mission to "protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation."[60] The agency was formed in the wake of the 1929 market crash:[61]

> The need for protective reform was pointed out clearly by the *House Report of the 73d Congress* which stated that "During the post war decade some 50 billion dollars worth of new securities were floated in the United States. Fully half or 25 billion dollars worth of securities floated during this period have proven to be worthless. These cold figures spell tragedy in the lives of thousands of individuals who invested their life savings, accumulated after years of effort, in these worthless securities . . . Alluring promises of easy wealth were freely made with little or no attempt to bring to the investors" attention those facts essential to estimating the worth of any security.[62]

The SEC protects investors by requiring disclosure of information material to their investment decisions. The theory is that armed with this information, they can make their own choices—good or bad—in a free and fair market.[63]

---

floor-of-this-national-security-investment/.

57. Jennifer Booton, *Three Reasons Why Cyberattacks Don't Hurt Stock Prices,* MARKETWATCH (Apr. 3, 2015), http://www.marketwatch.com/story/3-reasons-why-cyberattacks-dont-hurt-stock-prices-2015-04-03.

58. *See* SEC v. Rind, 991 F.2d 1486, 1490–92 (9th Cir. 1993) (describing the importance of material disclosure).

59. *Id.* at 1491.

60. SEC v. Wilson, No. 12-cv-15062 2012 U.S. Dist. LEXIS 165248 (E.D. Mich. Nov. 20, 2012) (quoting *The Investor's Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, SEC http://www.sec.gov/about/whatwedo.shtml (last visited Mar. 6, 2016)).

61. Lori A. Richards & John H. Walsh, *Compliance Inspections and Examinations by the Securities and Exchange Commission*, 52 BUS. LAW. 119, 120 (1996) (stating "[t]he Exchange Act . . . was enacted after the stock market crash of 1929 revealed shocking misconduct and marketplace anarchy").

62. Alan B. Levenson, *The Role of the SEC as a Consumer Protection Agency*, 27 BUS. LAW. 61 (1971).

63. *Id.* (stating that "[t]he economic justification for disclosure as the keystone of investor protection

> The laws and rules that govern the securities industry in the United States derive from a simple and straightforward concept: all investors, whether large institutions or private individuals, should have access to certain basic facts about an investment prior to buying it, and so long as they hold it. To achieve this, the SEC requires public companies to disclose meaningful financial and other information to the public. This provides a common pool of knowledge for all investors to use to judge for themselves whether to buy, sell, or hold a particular security. Only through the steady flow of timely, comprehensive, and accurate information can people make sound investment decisions.[64]

The securities laws, therefore, require public companies to report material information to the investing public; information is material if "there is a substantial likelihood that a reasonable investor would attach importance [to it] in determining whether to purchase the security."[65] "The SEC's reporting requirement is designed to provide investors with the information necessary to make informed decisions, and provides the SEC with a basis to police the actions of companies subject to the requirement."[66] The requirements of the SEC "are satisfied only by the filing of complete, accurate and timely reports."[67] These include quarterly and annual reports, in Forms 10-Q and 10-K,[68] as well as reports of extraordinary events as they occur, in Form 8-K.[69]

On Form 10-K, public companies must report, among other things:

- *Risk Factors.*[70] The report must discuss "the most significant factors that make the offering speculative or risky." Companies are not supposed to provide boilerplate disclaimers reporting generic risks that would affect all public companies. Instead, they are required to describe company or industry-specific risks.[71]
- *Management's Discussion and Analysis of Financial Condition and Results of Operations.*[72] In this section, management provides "information that the registrant believes to be necessary to an understanding of its financial condition, changes in

---

lies in the belief that material corporate and financial information disseminated to prospective investors provides a rational basis to evaluate securities and this is a necessary precondition to efficient markets").

64. *The Investor's Advocate*, *supra* note 60 ("The hiding and secreting of important information obstructs the operation of the markets as indices of real value . . . Delayed, inaccurate and misleading reports are the tools of the unconscionable market operator and the recreant corporate official who speculates on inside information . . . The reporting provisions . . . are a very modest beginning to afford that long delayed aid . . . in the way of securing proper information for the investors."); H.R. Rep. No. 73-1383, at 13 (1934).

65. 17 C.F.R. § 230.405 (2012); March Sadowitz, *Environmental Disclosure: What Is Required and What Is Needed*, 16 ENVTL. HIST. REV. 69, 70 (1992).

66. Abella v. Barringer Res., Inc., 615 A.2d 288, (N.J. Super. 1992).

67. SEC v. IMC Int'l, Inc., 384 F.Supp. 889, 893 (N.D.Tex. 1974); *See also* Abella v. Barringer Resources, Inc., 615 A.2d 288, 293 (N.J. Super. 1992) (describing qualified and conditional privilege).

68. 15 U.S.C. § 78m (2012); 17 C.F.R. §§ 240.13a-1, 13a-13 (2012).

69. 15 U.S.C. § 78m (2012); 17 C.F.R. § 240.13a-11 (2012).

70. 17 C.F.R. § 229.503(c) (2012).

71. *Id.*

72. 17 C.F.R. § 229.303 (2012).

financial condition and results of operations."[73] Management must "[d]escribe any unusual or infrequent events or transactions or any significant economic changes that materially affected the amount of reported income from continuing operations and, in each case, indicate the extent to which income was so affected."[74]

- *Business Description.*[75] This section includes descriptions of the company products, relationships with important customers and suppliers, and competitive conditions.[76]
- *Legal Proceedings.*[77] In the Legal Proceedings section, companies are required to briefly describe "any material pending legal proceedings, other than ordinary routine litigation incidental to the business . . ."[78]
- *Financial Statement Disclosures.*[79] SEC regulations state that financial statements "not prepared in accordance with generally accepted accounting principles are presumed to be misleading . . ."[80] "To meet the requirements of full disclosure," GAAP-compliant financial statements must have explanatory notes "to help users interpret some of the more complex items."[81] Material extraordinary charges must be individually explained.[82]

To ensure the integrity of the markets and the purchase-and-sale process, the SEC also has sweeping authority to demand records and to conduct compliance examinations of "national securities exchanges and their members," those selling securities, and other related entities.[83] The SEC Office of Compliance Inspections and Examinations (OCIE) focuses its "attention on the firms, and on the areas within firms, that need regulatory scrutiny the most."[84] There are four types of examinations conducted by OCIE: compliance examinations of regulated entities, oversight examinations of entities also regulated by a self-regulatory organization, inspections of the self-regulatory organizations themselves, and "special purpose, sweep, and cause examinations."[85]

During compliance and oversight examinations, the OCIE staff interview

73. *Id.*
74. *Id.*
75. 17 C.F.R. § 229.101 (2012).
76. 17 C.F.R. § 229.101(c) (2012).
77. 17 C.F.R. § 229.103.
78. *Id.*
79. Regulation S-X, 17 C.F.R. § 210 (2012).
80. 17 C.F.R. § 210.4-01 (2012).
81. BELVERD NEEDLES & MARIAN POWERS, FINANCIAL ACCOUNTING 50 (11th ed. 2011).
82. *See* William C. Norby, *Accounting for Financial Analysis: SEC Adopts an Activist Role in Accounting*, 28 FIN. ANALYSTS J. 96 (1972) (describing material charges).
83. 15 U.S.C. § 78q; SEC, OFF. OF COMPLIANCE INSPECTIONS & EXAMINATIONS, NAT'L EXAMINATION PROGRAM, EXAMINATION PRIORITIES FOR 2014 (Jan. 9, 2014) [hereinafter 2014 EXAMINATION PRIORITIES], https://www.sec.gov/about/offices/ocie/ national-examination-program-priorities-2014.pdf; Richards, *supra* note 61 at 132–33.
84. Richards & Walsh, *supra* note 61 at 147.
85. *Id.* at 136.

management, request documents for review and copying, and question knowledgeable employees.[86] Examinations result in a letter indicating whether the examiners found compliance failures or deficiencies.[87] If a deficiency letter is issued—and most examinations result in them—the OCIE follows up to ensure that the deficiencies are remedied. If they are not, an enforcement action may follow.[88]

Special purpose examinations are conducted in a similar manner, but are used to collect information from numerous entities at once on matters of particular concern to the SEC. "From time to time, the Commission, another division, or the examination staff determines that some development or market practice warrants special inquiry. Special purpose examinations are then used to gather the needed information on an expedited schedule. In sweep examinations, several teams conduct simultaneous examinations."[89]

2. SEC Response to Cybersecurity Risks

On October 13, 2011, the Securities and Exchange Commission, Division of Corporate Finance, issued "CF Disclosure Guidance: Topic No. 2 Cybersecurity."[90] The purpose was to provide "the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents."[91] Further reflecting the heightened concern of the SEC about cybersecurity, the Office of Compliance Inspections and Examinations—the self-described "'eyes and ears' of the SEC"—named cybersecurity as an examination priority in 2014 and 2015.[92]

a. 2011 Cybersecurity Disclosure Guidance

On May 11, 2011, five United States senators wrote to then-SEC Chairperson Mary Schapiro about their cybersecurity concerns.[93] Citing "inconsistencies in reporting, investor confusion, and the national importance of addressing cyberspace security," they urged the SEC to publish guidance "regarding the disclosure of information security risk including material network breaches."[94] The senators said it was "essential that corporate leaders know their responsibility for managing and disclosing information security

86. 2014 EXAMINATION PRIORITIES, *supra* note 83.
87. Richards & Walsh, *supra* note 61 at 143.
88. *Id.* at 140–46.
89. *Id.* at 136–37.
90. TOPIC NO. 2, *supra* note 7.
91. *Id.*
92. SEC, OFF. OF COMPLIANCE INSPECTIONS & EXAMINATIONS, NAT'L EXAMINATION PROGRAM, EXAMINATION PRIORITIES FOR 2015 at 3 (Jan. 15, 2015) [hereinafter 2015 EXAMINATION PRIORITIES], http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2015.pdf; 2014 EXAMINATION PRIORITIES, *supra* note 83, at 2.
93. Letter from Senator John D. Rockefeller, IV et. al. to Mary Schapiro, Chairperson of the United States Securities and Exchange Commission (May 11, 2011), http://commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e.
94. *Id.*

risk."[95]

The SEC responded on October 13, 2011 with CF Disclosure Guidance: Topic No. 2, Cybersecurity (Guidance).[96] It did not add to or modify existing disclosure requirements.[97] The "guidance" did not have the force of law; it did not go through the notice-and-comment procedure of a regulation.[98] However, it informed regulated parties how the SEC staff charged with enforcing the laws interpreted them.[99]

Noting that their increased reliance upon digital technologies had opened registrants to cyberattack, the agency said that reporting entities and professionals had become concerned about how to meet their disclosure obligations about this kind of risk.[100] The SEC said its response was aimed to be consistent with the disclosure requirements for any other type of business risk.[101]

The SEC emphasized (twice), however, that "detailed disclosures [that] could compromise cybersecurity efforts—for example, by providing a 'roadmap' for those who seek to infiltrate a registrant's network security— . . . are not required under the federal securities laws."[102] This assurance was cold comfort for, as one commentator put it, there was a "trade-off inherent in making Registrants' cybersecurity risks and prevention measures more transparent."[103]

> The trade-off can be summarized as follows: The more revealing a Registrant's cybersecurity disclosures become, the greater the likelihood that they will provide information useful to hackers and

95. *Id.*

96. TOPIC NO. 2, *supra* note 7; Roland L. Trope & Sarah Jane Hughes, *The SEC Staff's "Cybersecurity Disclosure" Guidance: Will It Help Investors or Cyber-Thieves More?*, AM. BAR ASS'N: BUS. L. TODAY (Dec. 19, 2011), http://www.americanbar.org/publications/blt/2011/12/03_trope.html ("On October 13, 2011, the SEC's Division of Corporate Finance quietly issued a new guidance . . . describing disclosures of cybersecurity incidents and attacks and the prevention and remediation measures that public companies . . . have suffered or may suffer, and of the prevention and remediation expenses they have expended or may expend . . . This Guidance is not a rule or a commission interpretation. It did not appear in the *Federal Register* for comment or otherwise. Its issuance is likely to cause substantial amounts of work among Registrants and legal professionals who represent them.").

97. Peter Romeo & Richard Parrino, *SEC Issues Guidance on Disclosure of Cybersecurity Risks and Cyber Incidents*, HOGAN LOVELLS SEC UPDATE (Oct. 25, 2012), http://www.hoganlovells.com/sec-issues-guidance-on-disclosure-of-cybersecurity-risks-and-cyber-incidents-10-25-2011/.

98. *See generally* 5 U.S.C. § 553 (2012) (describing the rule making process for federal regulations).

99. RESEARCHING THE FEDERAL SECURITIES LAWS THROUGH THE SEC WEBSITE, SEC http://www.sec.gov/investor/pubs/securitieslaws.htm (last modified Dec. 4, 2012) ("The Commission occasionally provides guidance on topics of general interest to the business and investment communities by issuing 'interpretive' releases, in which we publish our views and interpret the federal securities laws and SEC regulations. Interpretive releases . . . are not positive law but provide useful guidance as to the position of the SEC staff on various issues."); *see also* Romeo & Parrino, *supra* note 97 (discussing the ramifications of the SEC's cybersecurity disclosure guidance).

100. TOPIC NO. 2, *supra* note 7.

101. *Id.*

102. *Id.*

103. Trope & Hughes, *supra* note 96; Will Daugherty, *The Evolving Landscape of Cybersecurity Disclosures*, 23 SECUR. LIT. J. 6, 6 (Summer 2013) ("Providing detailed disclosures of cyberattacks can create the risk of providing a road map for future cyberattacks. Yet, a company's failure to adequately disclose cyber risks and incidents that have a material impact on the company's operations or financial condition may violate the federal securities laws.").

> competitors (Adversaries). Specifically, a Registrant's cybersecurity disclosures, which the longstanding SEC interpretations require be specific to the Registrant rather than generic, will be understood far better by a cyber Adversary, than by a potential investor, and, accordingly, more valuable to Adversaries . . . Registrants and their lawyers will not know, for a while at least, what the precise consequences of the new Guidance, intended and otherwise, will be. It also may take time for the SEC staff to discover how much value investors will gain from the required cybersecurity disclosures, or whether, as we fear, the earliest beneficiaries and the ones who stand the most to gain will be the Adversaries, not investors.[104]

The Guidance did not create any new reporting requirements, but made it "clear that the agency expect[ed] public companies . . . to have undertaken an assessment of the risks they face, the consequences that may occur in the occasion of a cyber event and how they might respond."[105] Rather than creating new requirements for cybersecurity, it took the approach of explaining how the old requirements applied to this new problem.

> The staff has typically handled new "disclosure areas" and "hot topics" by starting with the premise that our rules require disclosure of material information. So, our disclosure experts have provided guidance about how to address particular topics within the framework of providing information that is necessary for exercising an investment or voting decision . . . When the Commission adopted rules decades ago requiring a description of the company's business, risk factor disclosure and MD&A, there were no such things as smartphones, tablets, or even the internet. And, so it was not thinking about the risks presented by cybersecurity attacks or breaches. Even though cybersecurity attacks were not specifically contemplated, the disclosure requirements generally cover these risks. That is because, even in the absence of a line item requirement, the basic standard of "materiality" governs. Depending on the severity and impact of the cybersecurity attacks, disclosure is either required or not. And the staff of Corporation Finance, relying on the materiality standard, issued guidance in October 2011 to help companies work through the disclosure questions that arise when considering cybersecurity matters.[106]

Five 10-K report sections that might be affected by cybersecurity

---

104. Trope & Hughes, *supra* note 96; Howard M. Privette et al., *The SEC Guidance on Cybersecurity Measures for Public Companies*, L.A. LAW. Sept. 2014, at 14 ("Disclosure of cybersecurity problems by public companies . . . presents an interesting confluence of policy considerations for which there is still no consensus. On the one hand, investors may be interested in whether and to what extent a corporation may be burdened by cybersecurity expenses—whether they be the cost of building defenses or the losses arising from a breach. On the other hand, detailed discussion of the value of vulnerable assets or the reasons for their vulnerability may attract predators.").

105. Melissa Maleske, *Life's a Breach*, INSIDE COUNSEL (Dec. 29, 2011); *see also* Daughetry, *supra* note 103, at 6–7 (articulating the risks to investors from cybersecurity threats).

106. Mary Jo White, Chairwoman, SEC, Address at 2013 Leadership Conference of Nat'l Assoc. of Corp. Dir.: The Path Forward on Disclosure (Oct. 15, 2013), http://www.sec.gov/News/Speech/Detail/Speech/1370539878806#.VPTPHkun3cY.

incidents or risks were cited.[107] In the "Risk Factors" section, the Guidance said companies "should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky."[108] This did not sound new. It parroted the threshold definition of risk materiality in the regulatory instructions for 10-K reports.[109] Then, the agency spelled out what it expected for cybersecurity risks.[110] Companies were advised to evaluate cybersecurity risks by considering the frequency and severity of past events and the probability and magnitude of future incidents, including their financial and disruptive costs.[111] Companies were also instructed to factor in threats of attack, preventive measures, and insurance.[112] If, considering all these factors, management concluded the risk of a cybersecurity breach was material, necessary disclosures might include aspects of the business that were creating the risk and what the costs might be, risks related to outsourcing, descriptions of past cybersecurity breaches, risks of undetected breaches, and insurance coverage.[113]

Similarly, the "Management's Discussion and Analysis of Financial Condition and Results of Operations" (MD&A) section was to include "a discussion of cybersecurity risks and incidents if cyber incidents have had or are likely to have a material effect on a company's liquidity, results of operations or financial condition or would cause reported financial information not to be necessarily indicative of future operating result or financial condition."[114] Examples provided were the effects of intellectual property loss, a significant loss of customers following a cybersecurity breach, and materially elevated costs from remediation, litigation, or prevention.[115]

Likewise, the "Business Description" section was expected to include any cybersecurity breaches that affected the products, services, important customer or supplier relationships, or the ability to compete.[116] Disclosures might also be required in the "Legal Proceedings" section for actions relating to cybersecurity breaches, if the outcome could be material to the results of the company or in the "Financial Statement Disclosures" to explain extraordinary expenses, contingent losses, diminished cash flows, impairment of assets resulting from cybersecurity incidents or prevention tactics.[117]

In addition to these regular disclosures in annual 10-K reports, companies were required to report significant events as they occurred in a Form 8-K report "if necessary to maintain the accuracy and completeness of information

107. *Id.*
108. TOPIC NO. 2, *supra* note 7.
109. 17 C.F.R. § 229.503(c) (2011).
110. TOPIC NO. 2, *supra* note 7.
111. *Id.*
112. *Id.*
113. *Id.*; Elizabeth A. Ising & Alexander G. Acree, *SEC Issues Guidance on Cybersecurity Disclosures*, 25 INSIGHTS: CORP. & SEC. L. ADVISOR 34, 34–35 (2011).
114. *Id.*
115. TOPIC NO. 2, *supra* note 7.
116. *Id.*
117. *Id.*

in the context of securities offerings."[118] Companies were expected to disclose "the costs and other consequences of material cyber incidents" in an 8-K report.[119]

Although, in theory, the Guidance did not have the force of law, practitioners recognized that the failure to follow the "views" of the SEC staff could lead to an enforcement action.[120] As one attorney and former SEC staffer said,

> From my enforcement perspective, . . . these guidelines set up the situation where the SEC's going to bring an enforcement action against some company for making false or misleading statements about cybersecurity and exposure inside a major . . . company that failed to provide necessary notifications, and then experienced a massive breach. I can't say that tomorrow there will be an enforcement case, but the SEC doesn't write about stuff it's not concerned about.[121]

Close on the heels of the Guidance was the February 2012 justification for the Fiscal Year 2013 SEC budget.[122] In asking Congress for more funds, the SEC pointed to cybersecurity concerns.[123] "Financial entities are recognized as particular targets for cyber attack attempts. SEC monitoring of cyber security at the various securities exchanges and the growing number of trading and clearing platforms will require additional staff to further enhance this function in FY 2013."[124]

By the summer of 2012, staff reported that in reviews of 10-K reports, cybersecurity was an area of interest "particularly at companies that [had] been infiltrated."[125] In April 2013, the SEC was being pressured to make more stringent requirements and this was under review.[126] Applying "pressure on companies using . . . enforcement powers under existing disclosure requirements" was an additional possibility.[127]

By early 2014, practitioners reported that the SEC staff was regarding the Guidance with the force of a fully vetted regulation.[128] The SEC determined, based on the Guidance, that 2012 cybersecurity disclosures by six major

118. Ising & Acree, *supra* note 113, at 36.

119. *Id.*

120. Maleske, *supra* note 105.

121. *Id.*

122. SEC, IN BRIEF FY 2013 CONGRESSIONAL JUSTIFICATION, 6 (Feb. 2012), https://www.sec.gov/about/secfy13congbudgjust.pdf.

123. *Id.*

124. *Id.*

125. *Dialogue with the Director of the SEC Division of Corporation Finance*, 26 INSIGHTS: CORP. & SEC. L. ADVISOR 37, 37 (Sept. 2012).

126. Daugherty, *supra* note 103; Ernest Badway, *SEC Again Looking at Cybersecurity Issues*, SEC. COMPLIANCE SENTINEL (Oct. 28, 2013).

127. *Id.*

128. Gerry H. Grant & C. Terry Grant, *SEC Cybersecurity Disclosure Guidance Is Quickly Becoming a Requirement*, 84 CPA J. 69 (May 2014); Norah C. Avellan, Note, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 WASHBURN L.J. 193, 220–21 (2014).

publicly-traded companies did not go far enough.[129] "Requests" for additional information not honored could have resulted in sanctions or fines.[130] Moreover, according to some observers, the staff was ignoring the materiality requirement in the Guidance.[131]

> The SEC requested that Amazon disclose a cyber attack that stole millions of addresses and credit card information from its Zappos unit. Amazon eventually complied with the SEC's request, but only after arguing that the disclosure was not required because Zappos did not contribute material revenue. Hartford presented a materiality argument as well, but the SEC responded that any cyber attack should be disclosed.[132]

Commentators began urging the SEC to adopt the Guidance as a formal rule. In 2013, Senator John D. Rockefeller wrote to SEC Chairperson Mary Jo White that "given the growing significance of cybersecurity on investors' and stockholders' decisions, the SEC should elevate [the staff's] guidance and issue it at the Commission as well."[133] This, of course, would have subjected it to notice-and-comment procedure under the Administrative Procedure Act.[134] Chairperson White declined immediate action, "equating cybersecurity risks 'with other business risks' that should be 'among the factors a public company would consider in evaluating its disclosure obligations.'"[135]

The December 2014 spending bill required the SEC to report to the Appropriations Committees of the Senate and House of Representatives on efforts to modernize disclosure requirements, including those directed at cybersecurity.[136] The report was to be submitted within 90 days of passage of the bill.[137] Since then, there have been reports that the SEC has been weighing more stringent cybersecurity reporting requirements.[138] In June 2015, two more lawmakers pressed the SEC to require "regular disclosures from firms outlining their cyber practices, as well as a more consistent standard for Form 8-K disclosures following a successful cyberattack."[139]

---

129. Grant & Grant, *supra* note 128.

130. *Id.*

131. *Id.*

132. *Id.*

133. Letter from John D. Rockefeller IV, Chairman, Senate Comm. on Commerce, Sci. and Transp. to Mary Jo White, Chairperson, SEC (Apr. 9, 2013), http://www.privacyandsecuritymatters.com/files/2013/04/Rockefeller-SEC-letter.pdf; Howard M. Privette et al., *The SEC Guidance on Cybersecurity Measures for Public Companies*, L.A. L. 14, 15 (Sept. 2014).

134. 5 U.S.C. § 553 (2012).

135. Letter from Mary Jo White, Chairperson, SEC, to John D. Rockefeller IV, Chairman, Senate Comm. on Commerce, Sci. and Transp. (May 1, 2013), http://www.steptoe.com/assets/ attachments/4544.pdf; Privette, *supra* note 104, at 15.

136. H.R. Res. 83, 113th Cong. (2014) (enacted).

137. Jim Hamilton, *Spending Bill Funds SEC and CFTC, Amends Dodd-Frank Swaps Push-Out Provision*, SEC. REG. DAILY (Dec. 12, 2014), http://www.dailyreportingsuite.com/securities/news/spending_bill_funds_sec_and_cftc_amends_dodd_frank_swaps_push_out_provision.

138. Cory Bennett, *SEC Weighs Cybersecurity Disclosure Rules*, HILL (Jan. 14, 2015); Andrew Lustigman & Mason A. Barney, *Legal Landscape for Cybersecurity Risk Is Changing as Federal Government and SEC Take Action*, INSIDE COUNSEL (May 8, 2015), http://www.insidecounsel.com/2015/05/08/legal-landscape-for-cybersecurity-risk-is-changing.

139. Cory Bennett, *Lawmakers Want SEC to Force Detailed Cyber Disclosures*, HILL (June 18, 2015), http://thehill.com/policy/cybersecurity/245428-lawmakers-want-sec-to-force-detailed-cyber-disclosures.

b. Cybersecurity Examinations

In addition to spelling out how public companies should meet their disclosure obligations, the SEC has placed increasing emphasis on cybersecurity in its examinations of investment advisors and investment companies, broker-dealers, exchanges and self-regulatory organizations, and clearing and transfer agents.[140] In January 2014, the Office of Compliance Inspections and Examinations (OCIE) outlined twelve priority areas for its National Examination Program including "Technology," which, in turn, included "information security."[141] By April, cybersecurity was the subject of its own "Risk Alert" bulletin.[142] The OCIE declared that it planned to,

> conduct examinations of more than 50 registered broker-dealers and registered investment advisers focused on the following: the entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats."[143] The purpose of the examinations was to "help identify areas where the Commission and the industry can work together to protect investors and our capital markets from cybersecurity threats.[144]

Attached to the Risk Alert bulletin was a sample information request that OCIE might use in its upcoming examinations.[145] The request was highly detailed—28 requests, with as many as 14 subparts, some tracking the "Framework for Improving Critical Infrastructure Cybersecurity," released earlier in the year by the National Institute of Standards and Technology.[146] Selected broker-dealers would be required to disclose such information as:

- Which of a list of security practices a firm used, how often they were used, who was responsible for them, and if they were not used firm-wide, which parts of the firm did use them;
- A copy of the firm's information security policy;

---

140. These entities are subject to SEC cybersecurity requirements in Regulation S-P requiring them "to adopt written policies and procedures with administrative, technical and physical safeguards to protect customer records and information" and Regulation S-ID (requiring those regularly extending credit "to develop and implement written identity theft prevention programs designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.") Luke T. Cadigan & Sean P. Mahoney, *Developments in Cybersecurity Law Governing the Investment Industry*, 21 INVESTMENT L. 9–10 (2014).

141. 2014 EXAMINATION PRIORITIES, *supra* note 83, at 2.

142. RISK ALERT, *supra* note 8.

143. *Id.* at 2; Two weeks earlier, Commissioner Luis A. Aguilar told the Mutual Fund Directors Forum to "expect that SEC examiners will be reviewing whether asset managers have policies and procedures in place to prevent and detect cyber-attacks and whether they are properly safeguarding their systems against security risks." Luis A. Aguilar, Commissioner, SEC, Address at Mutual Fund Directors Forum 2014 Policy Conference: Taking an Informed Approach to Issues Facing the Mutual Fund Industry (Apr. 2, 2014), (transcript available at http://www.sec.gov/News/Speech/Detail/Speech/1370541390232).

144. RISK ALERT, *supra* note 8.

145. *Id.*

146. *Id.*

- Which of a list of network security practices a firm used; and
- The software or other method used to discover fraudulent attempts at customer transactions.[147]

"Cybersecurity" received its own heading in the "Examination Priorities for 2015."[148] The SEC expanded the prior year examination program directed at broker-dealers to include transfer agents in 2015.[149] Observers "expected that the SEC [would] expand its examinations to all U.S. public companies . . . ."[150]

In February 2015, after "the staff collected and analyzed information from . . . selected firms," the SEC released a summary of its findings.[151] In short, the SEC found, among other things, that of the 57 broker-dealers and 49 investment advisers examined: (1) most had been victims of cyberattacks; (2) the "vast majority . . . had adopted information security policies;" and (3) a smaller number—quite small in the case of investment advisers—applied their policies, periodic assessments, or training to vendors with access to their networks.[152]

c. Weaknesses in the SEC Response

The steps the SEC has taken suffer from serious shortcomings. For actual breaches, even though the Guidance reiterates the materiality standard, the SEC has required companies to disclose immaterial cyber incidents, which can cause either undue alarm or desensitization to events of true concern.[153] For cybersecurity risks, the Guidance does nothing to help investors evaluate the likelihood of a cyber incident with a material impact on operations.[154] Companies have responded to the Guidance with boilerplate language that fails to provide meaningful information.[155]

The OCIE cybersecurity examinations also pose a security risk. The SEC is gathering highly confidential information while its own system was recently criticized as insecure.[156]

147. *Id.* at app.

148. 2015 EXAMINATION PRIORITIES, *supra* note 92.

149. *Id.*

150. Stuart A. Krause et al., *Cybersecurity Insurance: It's Not Just for 'The Good Wife,'* CORP. COUNSEL (Feb. 5, 2015), http://www.corpcounsel.com/id=1202717092188/Cybersecurity-Insurance-Its-Not-Just-for-The-Good-Wife?slreturn=20150705005831.

151. SEC, OFF. OF COMPLIANCE INSPECTIONS & EXAMINATIONS, NAT'L EXAMINATION PROGRAM, CYBERSECURITY EXAMINATION SWEEP SUMMARY (Feb. 3, 2015), https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

152. *Id.*

153. SEC, DIV. OF INV. MGMT., *Cybersecurity Guidance* (Apr. 2015), http://www.sec.gov/investment/im-guidance-2015-02.pdf.

154. *Id.*

155. Joseph Menn, *Major Companies Keeping Cyber Attacks Secret from SEC, Investors Report*, INS. J. (Feb. 2, 2012), http://www.insurancejournal.com/news/national/2012/02/02/233863.htm.

156. Daugherty, *supra* note 103.

d. The Guidance Has Been Ineffective

Investors read about what appear to be major cybersecurity breaches in the news and want to know how they have or will affect publicly-traded companies. They also need to know how likely a company is to suffer a breach that will materially affect operations. The disclosures following the Guidance have not provided this information.

In 2012 and 2014, Yahoo!, Inc., an American multinational technology company known for its web portal and search engine experienced two significant breaches.[157] Information associated with approximately one-half million user accounts was stolen in July 2012 through two separate weaknesses in Yahoo's cybersecurity architecture.[158] In early 2014, Yahoo experienced a breach of its email customer information through mobile code, which exploited a programming language vulnerability and impacted advertisements on Yahoo's webpages.[159] Nevertheless, the Yahoo 10-K reports for the fiscal years 2012, 2013, and 2014 contain almost identical language.[160] Neither of the cybersecurity breaches is described.[161] The topics of outsourcing of countermeasure functions and the purchase of cybersecurity insurance coverage are not present.[162] In the Risk Factors section, Yahoo acknowledges that there have been past breaches and may be future breaches, which have or could cause certain types of harm.[163]

Other companies experiencing breaches have not been any more illuminating about them in their 10-K reports. Apple, Inc., an American multinational technology company that designs, develops, and sells electronics, software, and online services, also experienced two breaches: the first in 2012 and another in 2014. In September 2012, Apple device identifiers along with personal data of their owners were stolen and then published on the Internet.[164] Later in 2014, invaders accessed celebrity iCloud accounts by breaching Apple's authentication system.[165] The Annual Reports for 2012, 2013, and

157. Katherine Bindley, *Yahoo Password Check: Has Your Email Account Been Compromised?*, HUFFINGTON POST (July 12, 2012, 4:58 PM), http://www.huffingtonpost.com/2012/07/12/yahoo-password-email-hack_n_1669047.html; Jay Rossiter, *Important Security Update from Yahoo Mail Users*, YAHOO.TUMBLR.COM (Jan. 30, 2014), http://yahoo.tumblr.com/post/75083532312/important-security-update-for-yahoo-mail-users.

158. Bindley, *supra* note 157.

159. Rossiter, *supra* note 157.

160. Yahoo! Inc., Annual Report (Form 10-K) (Feb. 29, 2012), http://www.sec.gov/Archives/edgar/data/1011006/000119312512086972/d258337d10k.htm; Yahoo! Inc., Annual Report (Form 10-K) (Mar. 1, 2013), http://www.sec.gov/Archives/edgar/data/1011006/ 000119312513085111/d442073d10k.htm; Yahoo! Inc., Annual Report (Form 10-K) (Feb. 28, 2014), http://www.sec.gov/Archives/edgar/data/1011006/000119312514077321/d636872d10k.htm.

161. *Id.*

162. *Id.*

163. *Id.*; Yahoo! Inc. Annual Report (Form 10-K) (Feb. 27, 2015), http://www.sec.gov/Archives/edgar/data/1011006/000119312514077321/d636872d10k.htm.

164. Louis Goddard, *One Million Apple Device IDs with Personal Information Allegedly Stolen from FBI Laptop*, VERGE (Sept. 4, 2012, 9:22 AM), www.theverge.com/2012/9/4/3290789/antisec-fbi-udid-breach-iphone-ipad-apple.

165. Jacob Kastrenakes, *Apple Denies iCloud Breach in Celebrity Nude Photo Hack*, VERGE (Sept. 2, 2014, 2:41 PM), www.theverge.com/2014/9/2/6098107/apple-denies-icloud-breach-celebrity-nude-photo-hack.

2014 include the same general wording to describe business operations, cybersecurity issues, and the risks of breach.[166] The Form 10K reports that while a breach places customer relation and operations at risk, Apple has countermeasures in place to reduce the risk.[167] Facebook, Inc., the online social networking service experienced a breach of customer personal information during 2013.[168] While Facebook explains the reality of cybersecurity risks to customer relationships and operations, information describing the impact of the breach is not included in its 2013 or 2014 annual report.[169]

The reports of actual attacks, buried as they are with language about risk of future attacks, are further diluted because the SEC requires reports of immaterial cybersecurity events.[170] The Supreme Court recognized the effect of requiring insignificant information nearly forty years ago in *TSC Industries, Inc. v. Northway, Inc.*:[171]

> Some information is of such dubious significance that insistence on its disclosure may accomplish more harm than good . . . If the standard of materiality is unnecessarily low, not only may the corporation and its management be subjected to liability for insignificant omissions or misstatements, but also management's fear of exposing itself to substantial liability may cause it to simply bury the shareholders in an avalanche of trivial information—a result that is hardly conducive to informed decision making.[172]

Nevertheless, one commentator who studied correspondence between the SEC and ten large companies about cybersecurity observed "a kind of Kabuki exchange, in which the SEC would question the initial 10-K, the company would object to including more information because no attack has been material or materially adverse, the SEC would renew its request, and the company would concede, agreeing to include a sentence or two."[173] One such revised disclosure by the American International Group, Inc., acceptable to the

166. Apple Inc., Annual Report (Form 10-K), (Oct. 31, 2012), http://investor.apple.com/secfiling.cfm?filingid=1193125-12-444068&cik=; Apple Inc., Annual Report (Form 10-K), (Oct. 30, 2013), http://www.sec.gov/Archives/edgar/data/320193/000119312513416534/d590790d10k.htm; Apple Inc., Annual Report (Form 10-K), (Oct. 27, 2014), http://yahoo.brand.edgar-online.com/displayfilinginfo.aspx?FilingID=10264100-899-414610&type=sect&TabIndex=2&dcn=0001193125-14-383437&nav=1&src=Yahoo.

167. *Id.*

168. Facebook, Inc., Annual Report (Form 10-K), (Jan. 29, 2015), http://yahoo.brand.edgar-online.com/displayfilinginfo.aspx?FilingID=10436894-799-387648&type=sect&TabIndex=2&dcn=0001326801-15-000006&nav=1&src=Yahoo; Facebook, Inc., Annual Report (Form 10-K) (Jan. 31, 2014), http://yahoo.brand.edgar-online.com/displayfilinginfo.aspx?FilingID=9741731-748-413456&type=sect&TabIndex=2&companyid=673740&ppu=%252fdefault.aspx%253fcik% 253d1326801.

169. *Id.*

170. SEC, DIV. OF INV. MGMT., *Cybersecurity Guidance* (Apr. 2015), http://www.sec.gov/investment/im-guidance-2015-02.pdf.

171. 426 U.S. 438 (1976).

172. *Id.* at 448–49.

173. Matthew F. Ferraro, *"Groundbreaking" or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications*, 77 ALB. L. REV. 297, 335 (2013–14). The ten companies studied were Amazon.com, Inc., American International Group, Inc., Anheuser-Busch Inbev SA/NV, ConocoPhillips, Inc., Eastman Chemical Company, Google, Inc., Hartford Financial Services Group, Inc., Quest Diagnostics Inc., Verizon Communications, Inc., and Wyndham Worldwide Corporation. *Id.* at 324–35.

SEC, illustrates the problem: "Like other global companies, we have, from time to time, experienced threats to our data and systems, including malware and computer virus attacks, unauthorized access, systems failures and disruptions."[174] From this sentence, an investor cannot determine whether AIG is reporting a devastating hack of customer data or the annoying spam email that anybody using the internet receives.

In disclosures about the risk of future attack, reporting companies cannot be and have not been expected to provide damaging details about their cybersecurity weaknesses. There is no mechanism allowing an investor to judge the vulnerability of a company. Rather, the focus has been on the types of possible cyber breaches and the harms a company could suffer from them. Yahoo, for example, provides an informative qualitative description, but investors are left perplexed about their real question: The likelihood of a cyber invasion with a material effect on operations.[175]

> Our products and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information in our facilities and on our equipment, networks and corporate systems. Security breaches expose us to a risk of loss of this information, litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. Security breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure, increased remediation and other costs, damage to our reputation and a loss of confidence in the security of our products, services and networks that could have an adverse effect on our business. We take steps to prevent unauthorized access to our corporate systems, however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a triggering event, we may be unable to anticipate these techniques or implement adequate preventative measures. If an actual or perceived breach of our security occurs, the market perception of the effectiveness of our security measures could be harmed and we could lose users and customers.[176]

174. American International Group, Inc., Annual Report (Form 10-K) (Feb. 15, 2013), http://www.sec.gov/Archives/edgar/data/5272/000104746913001390/a2212976z10-k.htm.

175. Yahoo! Inc., Annual Report (Form 10-K) (Feb. 27, 2015), http://www.sec.gov/Archives/edgar/data/1011006/000119312514077321/d636872d10k.htm.

176. *Id.*

e. Problems with the Cybersecurity Examinations

Gathering information about the level of preparedness among broker-dealers through special purpose examinations is an appropriate regulatory exercise. The trouble is the SEC has demanded highly sensitive information and its own cybersecurity system is flawed.[177] The question is whether that system is responsible for keeping sensitive information protected.

i. The SEC Has Serious Flaws in Its Own Cybersecurity

The United States Government Accountability Office (GAO) 2014 Fiscal Year Audit Report cites weaknesses in the SEC's comprehensive security environment in two major areas: (1) maintenance and monitoring of configuration baseline standards; and (2) implementation of password setting and network service standards.[178] The appropriate management of these two areas is critical in defending against breaches. An adequate defense is manifested through a comprehensive security policy that addresses the network, hosts, access points, applications, and user procedures.

The GAO report cited as issue number one, "maintenance and monitoring of configuration baseline standards" and recommended that SEC security management address the need for a comprehensive approach in the identification and management of security for all hardware and software within its technology infrastructure.[179] After a management process is designed and implemented, most remaining aspects of configuration management are automated to speed the process of applying software patches to correct problems that have been identified as security issues.[180] Organizations without viable configuration management are not able to respond quickly to the discovery of security issues in system software. As a result, they are vulnerable to a cyber-attack that exploits that weakness.[181] In 2015, the University of Southern California experienced a cyber breach in which hackers took advantage of a known security issue on a server. The breach would not have been possible if the available software patch had been installed on the server. This breach had the potential of putting 30–40,000 student records containing personal information at risk.[182] Like USC, the SEC is not protecting its technology infrastructure through comprehensive configuration management and has placed its network, data, and programs at risk.[183]

177. Sarah N. Lynch, *U.S. SEC on the Prowl for Cyber Security Cases*, REUTERS (Feb. 20, 2015, 4:07 PM), http://www.reuters.com/article/sec-cyber-idUSL1N0VU2AV20150220.

178. U.S. GOV'T ACCOUNTABILITY OFF., REPORT TO CHAIR, SEC, INFORMATION SECURITY: SEC NEEDS TO IMPROVE CONTROLS OVER FINANCIAL SYSTEMS AND DATA (2014).

179. *Id.*

180. *Id.*

181. Dave Shackleford, *Secure Configuration Management Demystified* 3, SANS INST. (2012), https://www.sans.org/reading-room/whitepapers/analyst/secure-configuration-management-demystified-35205.

182. *Examples of Security Breaches and Corresponding Recommended Practices*, VIVA UNIV. (Sept. 2012), https://vivauniversity.files.wordpress.com/2012/09/examplesofsecuritybreach.pdf.

183. U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-387R, MGMT. REPORT: IMPROVEMENTS NEEDED IN SEC'S INTERNAL CONTROLS AND ACCOUNTING PROCEDURES (2015).

The GAO report cited as issue number two, "implementation of password setting and network service standards" and recommended that the SEC address the need for a comprehensive approach to managing both administrator and end-user accounts.[184] These accounts have different levels of access to and control over organizational networks, programs, and data. An administrator account has unlimited access.[185] Technical support staff know the user name and password of the administrator account and can perform any task through this account.[186] The elevated privileges of this account give the user full control over the system.[187] This control is needed to support the system but can be abused to cause a data breach, complete unauthorized transactions, or interrupt system service.[188] Cyber breaches caused by the exploitation of administrator accounts are involved in many data breaches.[189] Neither Edward Snowden's National Security Administration breach nor the Target breach of late 2013 could have been successful without the compromise and exploitation of the privileged credentials of administrator-type accounts.[190]

A comprehensive approach, following industry-tested standards, for end-user accounts is also critical.[191] The GAO audit reports that the SEC did not consistently implement strong password controls for identifying and authenticating users.[192] Weak login security credentials is considered the root cause of the Anthem breach.[193] Organizations, like the SEC, should take a proactive approach to protect the integrity and privacy of confidential corporate and customer-client information by answering key questions like "Who has access to what?" and "What did they do?"

ii. The SEC Is Asking for Highly Sensitive Information

The OCIE is gathering information about the level of preparedness among broker-dealers through special purpose examinations.[194] The examination's request for very detailed information is separated into several topics including:

---

184. *Id.*

185. J. MICHAEL BUTLER, SANS INST., PRIVILEGED PASSWORD SHARING: "ROOT" OF ALL EVIL 2 (2012) (explaining that administrator user accounts are also known as root, super user, and domain admin accounts).

186. DAVID J. JOHNSON, SANS INST., THE USE AND ADMIN. OF SHARED ACCOUNTS 14 (2012).

187. BUTLER, *supra* note 185.

188. *Id.*

189. *Id.*

190. Press Release, Cyberark, New Report: Advanced Cyber Attacks Reliant on Privileged Credential Exploitation (June 11, 2014), http://www.cyberark.com/press/new-report-advanced-cyber-attacks-reliant-privileged-credential-exploitation/; Brian Krebs, *Inside Target Corp., Days After 2013 Breach*, KREBSONSECURITY (Sept. 21, 2015), http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/.

191. *The CIS Critical Security Controls for Effective Cyber Defense*, CTR. FOR INTERNET SEC. (Oct. 15, 2015), https://www.cisecurity.org/critical-controls.cfm.

192. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 183, at 16.

193. Lance Whitney, *Anthem's Stolen Customer Data Not Encrypted*, CNET (Feb. 6, 2015), http://www.cnet.com/news/anthems-hacked-customer-data-was-not-encrypted/ ("Because an administrator's credentials were compromised, additional encryption would not have thwarted the attack.").

194. RISK ALERT, *supra* note 8 ("This document provides a sample list of requests for information that the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) may use in conducting examinations of registered entities regarding cybersecurity matters . . . . This document should not be considered all inclusive of the information that the OCIE may request.").

Identification of Risks/Cybersecurity Governance; Protection of Firm Networks and Information; Risks Associated With Remote Customer Access and Funds Transfer Requests; Risks Associated With Vendors and Other Third Parties; Detection of Unauthorized Activity; and the Other category for a wide range of information.[195] Much of the information in each of these categories is highly sensitive and could lead to a cybersecurity breach if accessed with criminal intent.[196]

Through the "Identification of Risks/Cybersecurity Governance" disclosure, the organization is revealing the details of how it has established and maintains cybersecurity policies governing its technology architecture.[197] An organization's technology architecture includes physical devices, software platforms, applications, data flow and storage, internal and external networking resources, and the user procedures.[198] Knowledge of the responsible personnel and the extent and timing of the inventory practices is highly sensitive. In general, cybersecurity breaches begin with reconnaissance.[199] Cyber attackers observe and probe an organization looking for entry and a plausible means to either disrupt the organization or steal information.[200]

To illustrate, a review of the information required in the OCIE examinations suggests the construction of a spear-phishing cyberattack in which the hackers would use social engineering tactics to gain access to an organization's technology resources.[201] From the insecure information obtained in the examination, hackers would learn the target personnel and could pose as an employee or vendor of the organization.[202] By revealing some highly sensitive information found in the examination report, the hacker would gain confidence of the target personnel.[203] The hacker would then request additional information or access privileges from the target personnel.[204] The Pentagon confirmed that its email system was breached through a spear-phishing attack aimed at one of its technology employees.[205]

The "Identification of Risks/Cybersecurity Governance" disclosure

195. *Id.* at 2.

196. *See id.* (highlighting sensitive categories where cybersecurity risk could exist for registered broker-dealers).

197. *Id.*

198. *See id.* (listing practices firms engage in for management of their information security).

199. Kelly Jackson Higgins, *How Lockheed Martin's 'Kill Chain' Stopped SecurID Hack*, DARK READING (Feb. 12, 2013), http://www.darkreading.com/attacks-breaches/how-lockheed-martins-kill-chain-stopped-securid-attack/d/d-id/1139125; Steve Hultquist, *Reconnaissance Is the Name of the Game in 2015*, SC MAG. (Jan. 1, 2015), http://www.scmagazine.com/reconnaissance-is-the-name-of-the-game-in-2015/article/390376/.

200. *Anatomy of Advanced Persistent Threats*, FIREEYE, https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html (last visited Mar. 6, 2016).

201. *See* FireEye, Inc., *Anatomy of a Spearphishing Attack*, YOUTUBE (Feb. 6, 2015), https://www.youtube.com/watch?v=2IUKrxVpw3M (describing cyberattacks where sophisticated hackers target individuals within an entity with privileged credentials using specifically tailored "bait" emails).

202. *Id.*

203. *Id.*

204. *Id.*

205. Tom Vanden Brook & Michael Winter, *Hackers Penetrated Pentagon Email*, USA TODAY (Aug. 7, 2015), http://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625/.

requests the description of "any findings from the most recent risk assessment that were deemed to be potentially moderate or high risk and have not yet been fully remediated."[206] This information is valuable in assessing an organization's ability to manage cybersecurity flaws because it identifies risks for which no countermeasure has yet been implemented.[207] It is also valuable for assessing weaknesses in an organization's technology infrastructure which can be used to initiate a cyber-attack.[208] This is the information needed by cyber-attackers to plan the entry and a plausible means to either disrupt the organization or steal information.[209]

Through the "Protection of Firm Networks and Information" disclosure, the organization identifies, if applicable, the standard model for its information security architecture and processes.[210] The disclosure also requests practices and controls regarding the protections of the organization's networks and information.[211] The first item on the list would catch the attention of a cyber-attacker: "written guidance and periodic training to employees concerning information security risks and responsibilities."[212] Employee activities generate the highest level of cybersecurity risk because they have detailed knowledge of the organization's operations and have access to its highly sensitive and valuable data.[213] The organization's guidance and periodic training of employees concerning information security and risks and responsibilities reveals the organization's posture on employee-generated cybersecurity risks.[214] For example, training related to the use of employee-owned devices on the company network along with document management guidelines are important to protect company operations and data.[215] Close evaluation of these practices can reveal weakness and provide the information needed by cyber-attackers.[216] Some organizations recognize the competitive advantage of employees conducting business operations without time and location restrictions.[217] Policies allowing the use of employee-owned devices support this agile computing environment, but special precautions and countermeasures are required to secure a processing environment that includes external devices.[218] It is not surprising that many organizations that allow

206. RISK ALERT, *supra* note 8 ("Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences.").

207. *See id.* (seeking information about firms' cybersecurity vulnerabilities).

208. *Id.*

209. FireEye, *supra* note 201.

210. RISK ALERT, *supra* note 8, at 2.

211. *Id.*

212. *Id.* ("Please indicate which of the following practices and controls regarding the protection of its networks and information are utilized by the Firm, and provide any relevant policies and procedures for each item.").

213. Rana Kanaan, *The Good, the Bad, and the Who-Knows About BYOD*, TECH.CO. (July 15, 2015, 11:00 AM), www.tech.co/good-bad-knows-byod-2015-07.

214. ERNST & YOUNG, *BRING YOUR OWN DEVICE SECURITY AND RISK CONSIDERATIONS FOR YOUR MOBILE DEVICE PROGRAM* (Sept. 2013), http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf.

215. *Id.*

216. *Id.*

217. Kanaan, *supra* note 213.

218. *Id.*

employee-owned devices to connect to the company network have experienced data breaches.[219] Through the information the SEC collected for its examination, the security management and policies for employee devices can be evaluated for weaknesses in protecting the organization from disruption and data breaches.

The disclosure topics "Risks Associated With Remote Customer Access and Funds Transfer Requests" and "Risks Associated with Vendors and Other Third Parties" address the cybersecurity exposure from providing external parties access to the internal network and sharing data.[220] Many organizations interact electronically with customers and suppliers, which builds and serves important relationships.[221] Operations are often designed so that the organization performs core competencies in-house and outsources remaining tasks.[222] Organizations implement an extranet, a secured private network that is accessed through Internet technology, to communicate and share data with customers and business partners.[223] Information the SEC collected about security weaknesses relating to third-party access could provide another path to cyber attack.

In late 2013, Target Corporation (Target) experienced a breach which resulted in the theft of 70 million customer debit and credit cards account information.[224] The breach was initiated when an HVAC vendor, using an authorized account, accessed Target's internal network and installed malware to collect the customer account information.[225] Target's supplier portal is accessible through a Google search and lists HVAC and refrigeration companies.[226] Cyber-attackers obtained access to Target's corporate network by compromising a third-party vendor.[227] The number of vendors compromised is unknown, but it only took one. Through a phishing email, an employee of the HVAC vendor installed the malware on the HVAC system.[228] Eventually, while accessing Target's network during a maintenance assignment at a Target site, the malware began the process of collecting Target's customer information.[229] Target's experience illustrates how an organization must protect the cybersecurity risk associated with its own technology architecture and the risk from all parties that interact with its

219. *Id.*

220. RISK ALERT, *supra* note 8.

221. Margot Slade, *BUSINESS TO BUSINESS; Sales? The Internet Will Handle That. Let's Talk Solutions*, N.Y. TIMES (June 7, 2000), http://www.nytimes.com/2000/06/07/business/business-to-business-sales-the-internet-will-handle-that-let-s-talk-solutions.html?pagewanted=all.EndFragment.

222. Laurie Collier Hillstrom, *Outsourcing*, REFERENCE FOR BUS. (2016), http://www.referenceforbusiness.com/encyclopedia/Oli-Per/Outsourcing.html.

223. Slade, *supra* note 221.

224. Meagan Clark, *Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed for the Giant Retailer*, INT'L BUS. TIMES (May 5, 2014, 11:39 AM), http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056.

225. Michael Kassner, *Anatomy of the Target Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015, 8:29 PM), http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

226. *Id.*

227. *Id.*

228. *Id.*

229. *Id.*

systems. The examination request detailed information on how an organization evaluates external parties. Much of the information is highly sensitive and could lead to a cybersecurity breach if accessed with criminal intent.

C. What the SEC Should Be Doing

Cybersecurity breaches clearly pose a risk to an organization and its investors. The SEC protects investors by requiring disclosure of information material to their investment decisions and by overseeing the purchase-and-sale process.[230] The means by which the SEC directs the disclosure of cybersecurity management information and oversees cybersecurity in the market process should not increase the cybersecurity risk. Publicly reporting cybersecurity management policy and storing sensitive examination information in insecure SEC technology infrastructure increase the risk of cyberattacks.[231] Requiring reports of immaterial cyber breaches drowns out reports investors really need. There are alternatives that would give investors the information they need without providing the "roadmap" to criminals the SEC wants to avoid.[232] *First*, for actual cybersecurity breaches, reports should only be required when the events are material and should be required to include specific information. *Second*, to evaluate risk for the investor, companies could obtain and then publicly report a rating from a cybersecurity auditor. This would be a voluntary program; companies could continue to report cybersecurity issues as currently required. *Third*, broker-dealers and other participants in the market process could also be audited for cybersecurity as needed at the insistence of the SEC.

Companies should not be required to report cybersecurity breaches that are immaterial. Forcing companies to make the general disclosure that they have been breached will not be meaningful to investors if immaterial breaches are included. In determining whether the breach needs to be disclosed, the questions should be: (a) whether the breach could have a material effect on the financial position or operating results of the company; or (b) whether the breach indicates a fundamental flaw within the company system that will be impossible, expensive, or time-consuming to fix.

The general definition of materiality under the securities laws is well-settled: a fact is material if "there is a substantial likelihood that a reasonable shareholder would consider it important"[233] and that an "omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."[234] The SEC has eschewed a

230. *The Investor's Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, SEC (last updated June 10, 2013), https://www.sec.gov/about/whatwedo.shtml.

231. *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH. (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

232. TOPIC NO. 2, *supra* note 7.

233. Basic Inc. v. Levinson, 485 U.S. 224, 231 (1988).

234. TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976).

quantitative bright-line approach to materiality in the context of numerical misstatements on financial filings,[235] but some have cited a rule of thumb of "five to ten percent or more."[236] Costs to remediate cybersecurity breaches can reach these numbers, but breaches can be material even if they do not.

A breach of cybersecurity, even if not immediately material in a financial sense (because of the size of the company or insurance coverage), can still be material if it compromises future business operations. A cyberbreach may expose a widespread problem in the comprehensive cyber security of an organization. Sony Corporation, which has annual revenues over $70 billion, suffered three system breaches during 2011 through the use of Structured Query Language (SQL) injections to extract information from databases using Web interfaces.[237] SQL injection attacks involve sending modified SQL statements to a Web application that, in turn, modifies a database.[238] Attackers send unexpected input through their Web browsers that enable them to read from, write to, and even delete entire databases.[239] SQL injection can even be used to execute commands on the server.[240] It is a common attack method for many high-profile attacks.[241]

Based on news reports, the Sony breaches were orchestrated by the hacktivist organizations LulSec and Anonymous as revenge for the "persecution" of George Holtz.[242] Holtz was being sued by Sony for circumventing its copyright protections and jailbreaking its PlayStation 3 platform.[243] The first attack occurred on April 17, 2011 when information from over 70 million accounts was stolen from the Sony PlayStation network.[244] The second occurred on May 1, 2011 when information from twenty-five million accounts was stolen from Sony Online Entertainment Services.[245] The third occurred on June 2, 2011 when information from one million accounts was stolen from Sony Pictures.com.[246] Sony's security

235. SEC, SEC STAFF ACCT. BULL.: NO. 99—MATERIALITY (Aug. 12, 1999), https://www.sec.gov/interps/account/sab99.htm.

236. SEC v. Antar, 15 F. Supp. 2d 477, 509 (D.N.J. 1998).

237. Cynthia Larose, *Once More into the Breach: Are We Learning Anything?*, WESTLAW J. BANK & LENDER LIAB. Aug. 1, 2011, https://privacyandsecuritymatters.mintzlevinblogs.com/wp-content/uploads/sites/6/2013/01/SonyCommentary_Larose1.pdf.

238. Tim Sammut & Mike Schliffman, *Understanding SQL Injection*, CISCO, http://www.cisco.com/c/en/us/about/security-center/sql-injection.html (last visited Mar. 6, 2016).

239. *Id.*

240. *Id.*

241. *Id.*

242. James Cook, *Here's Everything We Know About the Mysterious Hack of Sony Pictures*, BUS. INSIDER (Dec. 4, 2014), http://www.businessinsider.com/guardians-of-peace-hackers-sony-pictures-2014-12?r=UK&IR=T.

243. Sarah Jacobsson Purewal, *Sony Sues PS3 Hackers*, PCWORLD, http://www.pcworld.com/article/216547/Sony_Sues_PS3_Hackers.html (last visited Mar. 6, 2016).

244. Sebastian Anthony, *How the PlayStation Network Was Hacked*, EXTREMETECH, (Apr. 27, 2011, 9:07 AM), http://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked.

245. Charles Arthur, *Sony Suffers Second Data Breach with Theft of 25m More User Details*, GUARDIAN (May 3, 2011, 2:00 AM), http://www.theguardian.com/technology/blog/2011/may/03/sony-data-breach-online-entertainment.

246. *Sony's Hacking Woes Mount After PSN Breach (Roundup*), CNET (June 23, 2011, 7:34 AM), http://www.cnet.com/news/sonys-hacking-woes-mount-after-psn-breach-roundup/; Julianne Pepitone, *Group Claims Fresh Hack of 1 Million Sony Accounts*, CNN MONEY (June 2, 2011, 6:50 PM),

measures were not strong enough to stop the SQL injection attack by the attackers.[247] However, after each attack, Sony indicated that it had strengthened its security to prevent future attacks.[248] Although monetary costs of the attack might not be material, at least not immediately, the series of attacks demonstrated a cybersecurity weakness and an inability to recognize its seriousness that might alter the total mix for investors.

Accordingly, materiality for cybersecurity breaches cannot be measured purely by the numbers. Management should be required to consider other factors that might cause the breach to have a significant impact on business operations and reputation, such as: (1) whether information technology is the business of the company or its use is incidental to sales; (2) whether the breach resulted from a flaw that was immediately repaired or will require major revisions to the components of the technology infrastructure; and (3) whether the breach was a single event or was repeated.

If a cybersecurity breach was material, investors need more information about it than the Guidance suggests. Informing investors that a material breach occurred, without more, is insufficient; additional information is necessary to have the "total mix" of information.[249] Moreover, that information should be immediate. In a Form 8-K report, the company should be required to disclose the date and timeframe of the breach (e.g., over a three-week period in June 2015), a general description of the type of information affected (e.g., customer credit card numbers), the approximate magnitude of the breach (e.g., one million customers), the estimated cost of remediation (e.g., costs to repair the system flaw and credit repair services for customers), the applicable insurance coverage, management's evaluation of the difficulty in repairing the flaw, if it is not already repaired, and the anticipated effect on the reputation of the company. Companies should not be required to disclose precisely how the attack occurred, since that might compromise their own future security or, once the flaw is fixed, the systems of their competitors.

For risks of future attack, the approach should be different. In the Risk Factors section, investors need to know whether a company is financially prepared for a material cybersecurity incident and how likely such a breach is. With respect to financial preparedness, management should be required to discuss its insurance or reserving practices for cyber breaches. This will allow investors to judge how well-prepared a company is compared with others in the market for a cyber event without increasing the danger of its occurrence. It is the second type of information, the likelihood of a successful cyberattack, which can cause problems. Disclosing vulnerabilities is counterproductive; it

---

http://money.cnn.com/2011/06/02/technology/sony_lulz_hack/.

247. *See* Pepitone, *supra* note 246 (quoting the hackers "Lulz" website, "SonyPictures.com was owned by a very simple SQL injection.").

248. Larose, *supra* note 237 (detailing Sony costs and security tactics in the wake of the 2011 hackings, including "identity theft insurance for customers, improvements to network security, free access to content, customer support, and an investigation into the hacking incidents.").

249. Daugherty, *supra* note 103 ("While the guidance has had a positive impact on the information available to investors on [cyberattacks], the disclosures are generally still insufficient for investors to discern the true costs and benefits of companies' cyber security practices.").

is more useful to hackers than to most investors.[250] Certified cybersecurity auditors would provide investors with the information they need: whether the company is using state-of-the-art countermeasures to ward off attacks. Companies would disclose a cybersecurity grade rather than expose their security plans. This would avoid providing the "roadmap" for attack that the SEC says federal securities laws do not require.[251]

Retaining experts is not a new approach. The SEC has required or permitted reporting companies to retain outside experts to express opinions in their annual filings before.[252] Expert audits provide investors and the SEC itself, when it does not have in-house expertise or staff,[253] independent verification of complex matters that are material to company reports. For financial statements it is mandatory: financial statements of reporting companies must be audited.[254] Oil and gas companies have the option of retaining outside experts to oversee their reserves.[255] Those companies representing that their reserves are prepared or audited by a third party must file reports based on the Society of Petroleum Evaluation Engineer's audit report guidelines.[256]

An audit is a systematic process of objectively evaluating an aspect of an organization.[257] External accounting auditors are "authorized by law to examine and publicly issue opinions on the reliability of corporate financial reports."[258] "The U.S. Congress shaped the external auditing profession and created its primary audit objectives with the passage of the Securities Act of 1933 and the Securities Exchange Act of 1934."[259] SEC regulations promulgated under these laws require independent financial audits of all publically traded companies.[260] Accountants conducting these audits become

250. *See* Amy Terry Sheehan, *Meeting Expectations for SEC Disclosures of Cybersecurity Risks and Incidents (Part One of Two)*, CYBERSECURITY L. REP. 1 (Aug. 2015), http://www.davispolk.com/sites/default/files/agesser.Cybersecurity.Law_.Report.aug15.pdf ("Regulators like the SEC have to find the right balance between encouraging companies to be helpful with investors by accurately and fairly disclosing their risks, and helping sort out what is and what is not material for investors, while not requiring companies to provide a roadmap for hackers as to where they are vulnerable.").

251. TOPIC NO. 2, *supra* note 7.

252. *Id.*

253. At the highest level, of the four current SEC commissioners, three are lawyers and one is an economist; none has any expertise in cybersecurity or information technology. *See Current SEC Commissioners*, SEC (Sept. 17, 2013), https://www.sec.gov/about/commissioner.shtml (containing biographies accessed by clicking on pictures of commissioners). The SEC is currently seeking employees with expertise in "information security technology." *Invest in Your Career at the SEC*, SEC (Oct. 16, 2014), http://www.sec.gov/jobs/jobs_fulllist.shtml.

254. 17 C.F.R. pt. 210 (2015); United States v. Arthur Young, 465 U.S. 805, 819 n.15 (1984); *All About Auditors: What Investors Need to Know*, SEC (June 24, 2002), http://www.sec.gov/investor/pubs/aboutauditors.htm.

255. Paul R. Bessette et al., *Securities Litigation and the Energy Sector*, 33 ENERGY & MIN. L. INST. 10 (2012).

256. Modernization of Oil and Gas Reporting Requirements, 74 Fed. Reg. 2158 (Jan. 1, 2010) (to be codified at 17 C.F.R. pts. 210, 211, 229, 249).

257. *Audit*, NEW OXFORD AM. DICTIONARY 103 (2d ed. 2005), http://www.oxforddictionaries.com/us/definition/american_english/audit (last visited Feb. 15, 2016).

258. *Audits, External*, INC., *http://www.inc.com/encyclopedia/audits-external.html* (last visited Mar. 6, 2016).

259. *Id.*

260. *Id.*

familiar with the bookkeeping procedures of the client.[261] A final report to management often includes "recommendations on methodologies of improving internal controls."[262] External auditors compile an audit report, which formally sets forth the independent auditor's findings about the business's financial statements and conformity with generally accepted accounting principles.[263] The audit report includes an "opinion paragraph" which includes the auditor's formal announcement "on whether the statements are in accordance with generally accepted accounting principles."[264] A recommended approach for the external reporting of the cybersecurity management of an organization in order to disclose information about the risk to investors could be modeled after the external auditing practice of the organization's financial systems.

As an external auditor, a Certified Public Accountant (CPA) verifies the content of financial statements and the internal control over financial reporting.[265] The financial reporting-related information technology (IT) systems and data that are examined through the external auditing process are a subset of the aggregate systems and data an organization uses to support its overall business operations.[266] The financial accounting audit responsibilities do not encompass an evaluation of cybersecurity risks across the entire technology platform of an organization.[267]

To address these concerns for investors, stock companies could retain cybersecurity auditors to issue graded opinions. A cybersecurity auditor validates attainment of three security goals, referred to as the CIA Triad: confidentiality, integrity, and availability.[268] Confidentiality means that sensitive information cannot be read either while on a computer or traveling across a network.[269] Integrity means that attackers cannot change or destroy information in a computer or network without detection and that changed or destroyed information can be restored.[270] Availability means that people who are authorized to use information are not prevented from doing so by a computer or network attack.[271]

To verify that an organization is meeting these goals, the cybersecurity

261. *Id.*

262. *Id.*; AICPA, *Communicating Internal Control Related Matters Identified in an Audit*, OVERALL OBJECTIVES OF INDEPENDENT AUDITOR AU-C § 265 (2012).

263. *Audits, External*, *supra* note 258.

264. *Id.*

265. *Id.*

266. *See CAQ Alert #2014-3: Cybersecurity and the External Audit*, CTR. FOR AUDIT QUALITY (Mar. 21, 2014, 4:47 PM), http://www.thecaq.org/docs/alerts/caqalert_2014_03.pdf?sfvrsn=2 (stating "[t]he financial reporting-related information technology (IT) systems and data that may be in scope for the external audit usually are a subset of the aggregate systems and data used by companies to support their overall business operations and may be separately managed or controlled").

267. *See id.* ("The financial statement and ICFR audit responsibilities do not encompass an evaluation of cybersecurity risks across a company's entire IT platform.").

268. RANDALL J. BOYLE & RAYMOND R. PANKO, CORPORATE COMPUTER SECURITY 3 (4th ed. 2014).

269. *See* Ed Tittel, ABCS OF IT SECURITY FOR CPAS: A CPAS INTRODUCTION TO IT POLICIES AND PROCEDURES 2 (2008), https://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/CyberSecurity/DownloadableDocuments/ABCsSecurity2_PolicyProcedure.pdf (last visited Mar. 6, 2016) (describing the general application of the CIA's "confidentiality" tenet to cybersecurity).

270. *Id.*

271. *Id.*

auditor must examine the entire technology infrastructure including the network architecture, authentication systems, operating and application software systems, data management systems, and user procedures. Comprehensive security considers the strength of the cohesive operation of the security provisions in each component of the technology infrastructure. In addition, the cybersecurity auditor examines management policies and practices, including: assets management; human resources security; physical and environmental security; communications and operations management; access control policies; information systems acquisitions, development, and maintenance; information security incident management; business continuity management; and compliance.[272]

Cybersecurity breaches occur through vulnerability in the system security management of the technology infrastructure.[273] Many companies use one or more IT governance frameworks to guide them in developing a disciplined security management process because securing the technology infrastructure is too complicated to be managed informally.[274] A security management governance framework specifies the formal processes (planned series of actions) for planning, implementation, and oversight.[275] Several factors may motivate firms to formalize their security processes to minimize risk to their technology infrastructure. Motivators include: the high dependence on technology for business operation; direct and indirect expenses associated with cybersecurity incidence; and a growth in the number of compliance laws and regulations.[276] Many compliance regimes require firms to adopt a specific formal governance framework to drive security planning and operational management. [277] The most common governance frameworks include COSO, CobiT, and ISO/IEC 27000.[278]

The COSO and CobiT are self-certifying governance frameworks designed to guide implementation internally within an organization.[279] The Committee of Sponsoring Organizations of the Treadway Commission

272. *ISO/IEC 27002:2013: Information Technology, Security Techniques, Code of Practice for Information Security Controls*, ISO (Oct. 1, 2013), https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en.

273. *The Eight Most Common Causes of Data Breaches*, DARKREADING (May 22, 2013, 6:22 AM), http://www.darkreading.com/attacks-breaches/the-eight-most-common-causes-of-data-breaches/d/d-id/1139795 1139795; *see generally* SYLVESTER NGOMA, VULNERABILITY OF IT INFRASTRUCTURES: INTERNAL AND EXTERNAL THREATS (2012), http://www.congovision.com/IT-Security-Pub.pdf (describing general vulnerabilities commonly leading to cybersecurity breaches).

274. TED G. LEWIS, CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY: DEFENDING A NETWORKED NATION 8 (2014).

275. BUS. SOFTWARE ALLIANCE, INFORMATION SECURITY GOVERNANCE: TOWARD A FRAMEWORK FOR ACTION 5 (2003), https://www.entrust.com/wp-content/uploads/2013/05/ITgovtaskforce.pdf ("A governance framework is important because it provides a roadmap for the implementation, evaluation and improvement of information security practices. An organization that builds such a framework can use it to articulate goals and drive ownership of them, evaluate information security over time, and determine the need for additional measures.").

276. BOYLE & PANKO, *supra* note 268, at 65.

277. *Id.* at 116.

278. *Id.* at 111.

279. *The Committee of Sponsoring Organizations (COSO)*, CHI. ST. UNIV., https://www.csu.edu/internalaudit/cosoandcobit.htm (last visited Feb. 15, 2016).

(COSO) provides a general control planning and assessment tool to organizations for guidance on enterprise risk management, internal control and fraud deterrence, and reduce the extent of fraud in organizations.[280] The framework includes seventeen principles across the five components of internal control.[281] The framework focuses on process controls, which include the security management of these controls.[282] Control Objectives for Information and Related Technology (CobiT) is a framework for information technology (IT) management and IT governance.[283] CobiT is strongly preferred for the establishment of an organizations cybersecurity management policy by U.S. IT auditors because it was created by the ISACA, the primary professional association for IT auditors in the United States.[284] CobiT includes four domains: planning and organization; acquisition and implementations; delivery and support; and monitoring.[285] Like the COSO tool, the focus of the CobiT framework is on internal control.[286]

The ISO/IEC 27000 series consists of information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).[287] The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system.[288] The series design is broad in scope including privacy, confidentially, and IT security issues.[289] It may be applied to organizations independently of size or structure.[290] ISO/IEC 27001 specifies how to certify organizations as being compliant with the ISO/IEC 27002.[291] The focus of the ISO/IEC 27000 framework is specifications for an external review of an organization's system security management.[292]

---

280. *About Us*, COMM. SPONSORING ORGS. TREADWAY COMM'N, http://www.coso.org/ aboutus.htm (last visited Feb. 29, 2016).

281. J. STEPHEN MCNALLY, THE 2013 COSO FRAMEWORK & SOX COMPLIANCE: ONE APPROACH TO AN EFFECTIVE TRANSITION 5 (2013).

282. Ken Tysiac, *Align Your Controls with COSO's Principles*, J. ACCT. (Dec. 15, 2013), http://www.journalofaccountancy.com/news/2013/dec/20139279.html.

283. *What Is COBIT 5*?, INFO. SYS. AUDIT & CONTROL ASS'N, http://www.isaca.org/cobit/pages/default.aspx (last visited Feb. 29, 2016).

284. BOYLE & PANKO, *supra* note 268, at 114; *What Is COBIT 5?*, *supra* note 283; *About ISACA*, INFO. SYS. AUDIT & CONTROL ASS'N, http://www.isaca.org/about-isaca/Pages/default.aspx (last visited Feb. 29, 2016) ("[A]n independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.").

285. *Control Objectives for Information and Related Technology (COBIT)*, THE281GROUP, http://www.the281group.com/index.php/control-objectives-for-information-and-related-technology-cobit (last visited Mar. 6, 2016).

286. *Id.*

287. *An Introduction to ISO 27001*, *ISO 27002FalseISO 27008*, ISO 27000 DIRECTORY, http://www.27000.org (last visited Mar. 6, 2016) ("The ISO 27000 series of standards has been specifically reserved by ISO for information security matters.").

288. *ISO 2700 Series Security Standards*, CASTLE FORCE IT SEC., http://www.castleforce.co.uk/Compliance/ISO27001.aspx (last visited Feb. 29, 2016).

289. *Id.*

290. *Id.*

291. *Id.*

292. BOYLE & PANKO, *supra* note 268, at 116.

The cybersecurity auditors, following the ISO/IEC 27000 framework's specifications on the verification of an external review of an organization's system security management, will become acquainted with flaws in cybersecurity management policies and procedures. The final report to management should include recommendations for improving the cybersecurity controls. The external cybersecurity auditor should issue an audit report that formally sets forth the independent auditor's findings about the business' cybersecurity management policy and the level of conformity with the ISO/IEC 27000 framework. The audit report includes an *opinion paragraph*, which includes the auditor's formal announcement on whether the organization is in accordance with ISO/IEC 27000 framework. Various audit opinions should be defined which indicate that the organization confirms or does not confirm. The opinions should be worded so that they reveal neither the specifics of the organization's cybersecurity policy nor any particular vulnerability. The opinions could be issued in accordance with a rating system.

External auditors certified in cybersecurity management could be authorized by law to examine and publicly issue opinions on the reliability of the cybersecurity management of a business. Cybersecurity auditors typically hold certifications to validate their expertise.[293] Internationally recognized certifications of IT audit competency include the Certified Information Systems Auditor (CISA) credential by ISACA and the Certified Information Systems Security Professional (CISSP) backed by ISC, the globally recognized organization dedicated to advancing the information security field.[294] Both certifications meet the ISO/IEC Standard for information security.[295]

If cybersecurity audits were required for all publicly traded companies, initially, there would not be enough experienced CISAs and CISSPs to go around. Although there are about 100,000 CISAs[296] and 100,000 CISSPs[297] worldwide as of 2015, most have careers within industry and not in auditing.[298] The program would have to be voluntary and companies would have the alternative of disclosing cybersecurity issues as currently required. As the cybersecurity grade becomes accepted by investors, their market behavior would encourage companies to have their cybersecurity systems audited. The role of the SEC would be to establish a standardized grading system, in conjunction with the ISO and IEC, which would provide consistent and meaningful information to investors when companies choose to be audited. The grading system would give investors the information they need about risk without increasing the exposure of reporting companies.

---

293. Kevin Beaver, *Best Practices for Choosing an Outside IT Auditor*, TECHTARGET (Sept. 2004), http://searchsecurity.techtarget.com/tip/Best-practices-for-choosing-an-outside-IT-auditor.

294. *Id.*

295. *Id.*

296. *Certified Information Systems Auditor (CISA) Fact Sheet*, INFO. SYS. AUDIT & CONTROL ASS'N, http://www.isaca.org/About-ISACA/Press-room/Pages/CISA-Fact-Sheet.aspx (last visited Mar. 6, 2016).

297. *(ISC)² Member Counts*, (ISC)², https://www.isc2.org/member-counts.aspx (last visited Mar. 6, 2016).

298. Certified Information Systems Auditor, *supra* note 296.

Similarly, cybersecurity auditors could be used to assess the preparedness of the purchase-and-sale process, such as broker-dealers, transfer agents, and the markets themselves. Rather than conduct this function in-house where it has its own security problems, the SEC could entrust this function to cybersecurity experts whenever the agency determined that such an examination was necessary. This would permit the SEC to obtain the information necessary to gauge cybersecurity risks to the markets and its operators without adding to those risks through the examination process.

III. CONCLUSION

Startling headlines about cybersecurity breaches are a matter of concern to investors in publicly-traded companies. The types of information involved, the methods of breaching security, and the number of people affected vary widely. Protection is only as strong as the weakest link—the company must protect against every imaginable way in, since the hacker only needs to find one opening. To date, the impact on share price has been delayed while the effects of the breach are measured, but stock price has reacted negatively once the costs of remediation emerge.[299]

The SEC is charged with protecting investors by (1) requiring public companies to disclose information material to their investment decisions; and (2) ensuring the integrity of the markets themselves through examinations of broker-dealers, exchanges, and others involved in the selling process.[300] Regarding cybersecurity, the agency spelled out what companies are expected to disclose under existing requirements.[301] It also stressed that the securities laws did not require companies to give hackers a roadmap.[302] Its Guidance, however, has yielded useless boilerplate disclosures from the companies addressing the subject at all. In some cases, the SEC has demanded that individual companies follow up with immaterial information more likely to confuse investors.

The SEC has also conducted a special purpose sweep examination of broker-dealers to assess their preparedness for cyberattacks, requiring detailed, specific information about methods used to ward them off.[303] Because the SEC has its own cybersecurity flaws, questions arise as to whether the information it collects is kept secure.

The SEC has an important role in making sure investors have the information they need about company cybersecurity risks and incidents and in ensuring the markets themselves operate free of cyber vandalism. The approach taken to date, however, needs to be substantially reworked. Cybersecurity breaches should not have to be reported unless they are material

299. Sebastien Gay, *Strategic News Bundling and Privacy Breach Disclosures* 4, U.S. FED. TRADE COMM'N (unpublished manuscript) (Aug. 21, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/09/00017-97599.pdf.

300. *The Investor's Advocate*, *supra* note 230.

301. RISK ALERT, *supra* note 8.

302. *Id.*

303. CYBERSECURITY EXAMINATION SWEEP SUMMARY, *supra* note 151.

to the company, either financially or to business operations or reputation. If they are material, then specific information should be required in a Form 8-K report. The risk of future breaches should be treated differently. The agency should adopt rules permitting reporting companies to disclose ratings from outside cybersecurity auditors and should use such certified auditors to collect information about broker-dealers and others involved in the purchase-and-sale process. This would provide the market and the SEC with the information they need without disclosing specific weaknesses to those who would exploit them. Finally, to assess cybersecurity readiness among securities markets and those involved in the purchase-and-sale process, the SEC should retain cybersecurity auditors to perform examinations rather than collect highly sensitive information in-house.