Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 14 | Issue 2 Article 1

6-22-2020

THE CRIMINAL, REGULATORY, AND CIVIL ISSUES SURROUNDING INTELLECTUAL PROPERTY AND CYBERSECURITY

Ernest Edward Badway

Christie McGuinness

THE CRIMINAL, REGULATORY, AND CIVIL ISSUES SURROUNDING INTELLECTUAL PROPERTY AND CYBERSECURITY

Ernest Edward Badway[*] *& Christie McGuinness*[**]

ABSTRACT

Cyber-attacks have affected all organizations and individual consumers. Dissemination of relevant information and attention to strong information security practices is an important tool in fighting this cyber "pandemic." Additionally, the legal and regulatory liability companies face from cyber-attacks as well as general strategies and practical solutions companies may implement to protect against cyber-intrusions and respond effectively in the event of an attack are considered. There are many iterations of cyber-crime, and we address the various methods cybercriminals use and the many ways cyber-attacks can take place, as well as the entities and victims affected. Moreover, the legal liability and regulatory oversight these entities face is a critical factor in addressing strategies and solutions, including both preemptive and response-oriented measures companies must take to combat cyber-crime. Coupled with this very active problem is the present nadir in the congressional debate and the proposed solutions. Thus, this Article suggests a comprehensive set of proposals where, if applied, companies may fortify their abilities to ward off cyber-threats and better ensure that consumers' personal information stays protected. Finally, these proposals would incentivize prompt cybersecurity responses and ensure adequate protection of company and consumer information.

INTRODUCTION

While the shift that our society has taken towards digitization increases its exposure to cyber-attacks, not all organizations and individual consumers appreciate the importance of strong information security practices.[1] This

---

* Mr. Badway is partner with and chair of the Securities Industry Group of Fox Rothschild LLP in New York, New York, and Morristown, New Jersey, as well as a former SEC Enforcement attorney, and an Adjunct Assistant Professor of Law at Brooklyn Law School. Mr. Badway would also like to thank his partner, Frank C. Razzano, Esq., for his research guidance regarding this Article as well as his current and past research assistants, David W. Inkeles and Yuliya Zahoroda, for their assistance in the research of this Article.

** Ms. McGuinness is an associate at Saul Ewing Arnstein & Lehr, LLP, and graduate of Brooklyn Law School.

1. Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 151 (2005); *see also* Robert S. Mueller, III, Dir., Fed. Bureau of Investigation, RSA Cybersecurity Conference in San Francisco, CA (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies ("I am convinced that there are only two types of companies: those that have been hacked and those that will be.").

Article discusses cyber-crime focusing on the legal and regulatory liability companies face from cyber-attacks. General strategies and practical solutions companies may implement to protect against cyber-intrusions and respond effectively in the event of an attack are also addressed.

Cybersecurity attacks are costly, increasingly prevalent, and have recently inspired congressional debate regarding appropriate solutions. A 2014 report, conducted by the Ponemon Institute, found that nearly half the companies surveyed had experienced a data breach in the previous year.[2] Another study, conducted the same year, figured that the annual cost of cybercrime was $445 billion.[3] The current legislative debate has focused on bills that would shield data sharing between companies, and with the government, from liability.[4] The Obama administration even set out voluntary guidelines designed to present a framework of best practices for preventing cyber-attacks.[5] These are steps in the right direction, but stronger protections are needed.

Part I of this Article begins with an overview of the many iterations of cyber-crime. Any such discussion must address the various methods cybercriminals use and the many ways cyber-attacks can take place, as well as the entities and victims affected. Additionally, Part I discusses the legal liability and regulatory oversight these entities face. Part II of this Article introduces strategies and solutions. These include both preemptive and response-oriented measures companies must take to combat cyber-crime. Part III provides a discussion of the present congressional debate and the proposed solutions. In adopting the comprehensive set of proposals outlined in the Article, companies may fortify their abilities to ward off cyber-threats and better ensure that consumers' personal information stays protected.

This Article recommends a series of proposals that incentivize prompt cybersecurity responses and ensure adequate protection of company and consumer information. Specifically, Congress must pass a comprehensive law allowing for data sharing between companies and the government; federalize a data breach notification standard that replaces the varying state notification laws; and the Securities Exchange Commission (SEC or the

2. Elizabeth Weise, *43% of Companies Had a Data Breach in the Past Year*, USA TODAY (Sept. 24, 2014), http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/.

3. Ellen Nakashima & Andrea Peterson, *Report: Cybercrime and Espionage Costs $445 Billion Annually*, WASH. POST (June 9, 2014), https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html.

4. Eric Naing, *Congress Urged to Pass Cyber Sharing Protections*, CQ ROLL CALL, June 29, 2015, 2015 WL 3939507.

5. *See* Exec. Order No. 13691, 3 C.F.R. § 13691 (2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (describing the specific methods for sharing cybersecurity information in the private sector).

Commission) must clarify its disclosure guidelines relevant to cybersecurity threats and incidents.

I. THE MANY ITERATIONS OF CYBERCRIME

A. THREATS

1. Hacking and Data Breaches

A data breach is essentially any infiltration of an information technology system, which is commonly accompanied by theft of sensitive personal data.[6] A hacker[7] is defined as any person who "uses computers to gain unauthorized access to data."[8] A data breach can range from unauthorized access—hacking—of a computer network to the theft of portable computers or storage devices by an employee, or others.[9]

Once a cybercriminal penetrates a computer network, the hacker can engage in a number of nefarious acts. The attacker can purloin customer information to commit fraud, install malicious software to carry out further attacks, or simply disrupt service to the target site. Even in the absence of theft of customer data or immediate harm to a network system or site, cyber-attacks pose significant reputational damage to targeted companies.[10] The following subsections will describe some of the major tactics cybercriminals use to carry out their attacks.

a. Phishing

Hackers frequently rely on phishing to perpetuate high-profile data breaches.[11] "Phishing," as defined by the Department of Justice (DOJ), refers to deceptive practices used by cybercriminals to pilfer—or "fish for"—personal information.[12] Usually, the cybercriminal will craft and send a fake e-mail disguised as business or organization that has a pre-existing

6. *See, e.g.*, Caroline C. Cease, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 396–97 (2014) (describing the common underlying sequence of events in a typical data breach action).

7. Throughout this Article the terms "hacker," "cybercriminal," and "attacker" will be used interchangeably. These terms will refer to individuals or group actors who create, find, and infiltrate vulnerabilities in information security networks.

8. Michael Preciado, *If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Government to Protect Critical Infrastructure from Cyber Warfare*, 1 J.L. & CYBER WARFARE 99, 110–11 (2012).

9. Cease, *supra* note 6, at 396.

10. Matwyshyn, *supra* note 1, at 138–39.

11. *See* Kristin Shields, *Cybersecurity: Recognizing the Risk and Protecting Against Attacks*, 19 N.C. BANKING INST. 345, 346 (2015) ("For over a decade, cybercriminals have been . . . 'phishing,' to steal customers' identification and account information.").

12. U.S. DEP'T OF JUSTICE, REPORT ON PHISHING 3 (2006), http://www.justice.gov/sites/default/files/opa/legacy/2006/11/21/report_on_phishing.pdf.

relationship with the recipient.[13] The cybercriminal deceives the recipient into clicking on a link to a phony website.[14] If the phishing attempt is successful, the victim will enter personally identifiable information on the belief that the message and site are legitimate.[15] Once the hacker has access to the information, the cybercriminal can use it to commit fraud.[16] Attacks on JP Morgan Chase and Sony Corporation indicate that phishing is perhaps one of the most commonly used, and effective, cyber-threats facing businesses and their customers.[17]

b. Malware and Spyware

Once a hacker gains unauthorized access to a network or computer, perhaps after a successful phishing expedition, it can install "malware," or malicious software. Hackers install malware on unsuspecting computers, phones, or similar devices.[18] This software is used to further exploit vulnerabilities in a company's information technology (IT) network. Malware is used to further many of the same criminal aims as phishing, such as stealing personal information, sending spam, and committing fraud.[19] "Spyware" is a close cousin of malware. It generally refers to software that is installed without authorization to monitor activity and mine information to send to a remote third-party.[20]

c. Denial of Service Attacks

In a denial of service (DoS) attack, cybercriminals swamp servers with information to disrupt the target's website. In its barest form, a single person with ample computing resources can carry out a DoS attack by overwhelming

13. The e-mail, purportedly from a bank, for example, might threaten to close an account or take other action if the recipient does not respond. *How to Recognize and Avoid Phishing Scams*, FED. TRADE COMM'N (May 2019), http://www.consumer.ftc.gov/articles/0003-phishing.

14. Although it may be a link to a phony website, there are other tactics employed as well; for instance, an email may direct someone to send banking information to prevent a friend or loved one from being harmed, or offer a reward for "answering a few simple questions" that turn out to be nothing more than a scheme to obtain personal information to be used by the cybercriminal.

15. *Id.*

16. Once a customer's information is stolen, the cybercriminal can use that data to make purchases, withdraw money from existing accounts, or open up phony bank or credit accounts in the victim's name. Lauren L. Sullins, *"Phishing" for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft*, 20 EMORY INT'L. L. REV. 397, 402–03 (2006).

17. *See* Jeffrey Roman, *Chase Breach Affects 76 Million Households*, BANKINFOSECURITY (Oct. 2, 2014), https://www.bankinfosecurity.com/chase-breach-affects-76-million-households-a-7395; *see also* Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED (Dec. 3, 2014), https://www.wired.com/2014/12/sony-hack-what-we-know/.

18. *Malware*, FED. TRADE COMM'N (Nov. 2015), https://www.consumer.ftc.gov/articles/0011-malware.

19. *Id.* Malware and phishing often go hand in hand. For instance, malware was installed on unsuspecting devices in a phishing attack against JP Morgan. Shields, *supra* note 11, at 350.

20. Daniel B. Garrie et al., *The Legal Status of Spyware*, 59 FED. COMM. L.J. 157, 160 (2006).

a target site with meaningless connections until it is rendered inaccessible.[21] Typically, however, these attacks are orchestrated as distributed denial of service (DDoS) campaigns.

A DDoS attack begins when one user gains control over multiple computers, or "zombies," through phishing or the installation of malware.[22] Once "recruited," these zombie computers are then summoned by the perpetrator to wage a large-scale DoS attack on the server.[23] The primary goal of such an attack is to shut down the target network. Still, absent a full shut down, an effective attack might result in blocking out or diverting legitimate users from the target site.[24]

d. Third-Party Vendor Attacks

To circumvent a target company's cybersecurity defense systems, criminals will set their sights on third-party vendors. Third-party vendors include law firms, marketing companies, or other merchants. Usually, they are companies that frequently contract with the target for specified transactions or purposes. The nature of these relationships requires the disclosure and transmission of significant customer information. Accordingly, many hackers will hone in on attacking these vendors' systems rather than directly trying to infiltrate a target company that is more attuned to the risks associated with these hacks and has focused more on cyber-protection.

Hackers can also use third-party vendors' credentials to commit a phishing attack on the target company. This was the tactic employed by criminals against Home Depot in 2014, who attempted to enter the company's network with a fake third-party vendor username and password.[25] Third-party vendors remain a viable entry point for cybercriminals to carry out large-scale data breaches.[26]

e. "Dumpster Diving"

Traditional dumpster diving is hacking in its most classical sense. Criminals search through trash receptacles behind corporate offices looking for discarded hard copies of documents. The goal, like many electronic data

21. *See* Joseph Menn, *Cyber-Attacks Against Banks More Severe than Most Realize*, REUTERS (May 18, 2013, 11:18 AM), http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518; W. Cagney McCormick, *The Computer Fraud & Abuse Act: Failing to Evolve with the Digital Age*, 16 SMU SCI. & TECH. L. REV. 481, 487–88 (2013).

22. Joshua McLaurin, *Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks*, 30 YALE L. & POL'Y REV. 211, 216–17 (2011).

23. *Id.*

24. McCormick, *supra* note 21, at 487–88.

25. Press Release, The Home Depot, The Home Depot Reports Findings in Payment Data Breach Investigation (Nov. 6, 2014), https://ir.homedepot.com/news-releases/2014/11-06-2014-014517315.

26. *Id.*

breaches, is to steal sensitive customer or company information to perpetuate fraudulent transactions.[27] While not nearly as sophisticated as the cyber-attacks discussed above, traditional dumpster diving nevertheless remains a risk that companies should not overlook.[28]

"Dumpster diving" in the cyber context refers to the unauthorized rummaging through company-owned servers, computers, or e-mail accounts for secret or discarded information.[29] This tactic often occurs in the employment context. An insider—employee or independent contractor with at least limited access to company information—will prowl old folders, e-mail accounts, and other internal documents for sensitive intellectual property (typically trade secrets) or customer information.

2. Employment Issues—Economic Espionage and Trade Secret Misappropriation

Many corporate assets derive value as a result of their confidential nature. Customer information, preference databases, and trade secrets, if poached or simply discovered, may significantly reduce the value of a company's intellectual property assets. Employees are in a unique position to access these assets and therefore present opportune entry points for many cybercriminals. Companies must consider protections against these 'inside jobs' with the same degree of care as they treat sophisticated cyber-attacks from outsiders.[30] Both the Target Corporation and JP Morgan data breaches used employees as initial targets. In the Target breach, the cybercriminals hacked a contractor's credentials;[31] in the JP Morgan attack, the hacking began by gaining access to the personal computer of an employee working from home.[32]

Employees are also capable of economic espionage, which is intentionally stealing data or misappropriating company trade secrets for

27. *Dumpster Diving*, TECHOPEDIA (July 19, 2012), https://www.techopedia.com/definition/10267/dumpster-diving.

28. *See* Thomas W. Tedford, *Dumpster Divers Could Be the Next Sony Hackers*, RECODE (Mar. 10, 2015), http://recode.net/2015/03/10/dumpster-divers-could-be-the-next-sony-hackers/ (discussing the risks of traditional dumpster diving to companies).

29. TECHOPEDIA, *supra* note 27.

30. The recent theft of trade secrets from Avago Technologies and Skyworks Solutions Inc. by state-actors masking as employees highlights the threat of economic espionage. Andrew Grossman, *U.S. Charges Six Chinese Citizens with Economic Espionage*, WALL ST. J. (May 19, 2015), http://www.wsj.com/articles/u-s-charges-six-chinese-citizens-with-economic-espionage-1432046527.

31. Jessica Silver-Greenberg & Matthew Goldstein, *After JPMorgan Chase Breach, Push to Close Wall St. Security Gaps*, N.Y. TIMES (Oct. 21, 2014), http://dealbook.nytimes.com/2014/10/21/after-jpmorgan-cyberattack-a-push-to-fortify-wall-street-banks/?_php=true&_type=blogs&_r=0.

32. Emily Glazer & Danny Yadron, *J.P. Morgan Says About 76 Million Houses Affected by Cyber Breach*, WALL ST. J. (Oct. 2, 2014), http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372.

their own benefit.[33] A trade secret is defined as information—such as a formula or compilation of data—that derives its economic value from not being readily ascertainable through proper means by those who could gain value from its use or disclosure.[34] To gain trade secret protection, the company must show that it took reasonable efforts to maintain the secrecy of the information.[35] Moreover, misappropriation of a trade secret in the employment context requires showing a duty of confidentiality followed by a breach. This is necessary both to protect information as a trade secret and to succeed in a potential misappropriation action. Indicia of secrecy include non-disclosure agreements, limitations on access, internal memos, trainings, and other precautions.

B. ENTITIES AT RISK

1. Financial Institutions

Financial institutions are frequent targets of cyber-attacks. In February 2015, Kaspersky Lab, a Russian cybersecurity company, released a report detailing an alleged $1 billion cyber-heist of 100 banks from around the globe.[36] The report, which withheld publication of the victim-banks' names due to nondisclosure agreements,[37] cited phishing attacks followed by the installation of malware on employees' computers as the entry points for the attacks. Prior to these attacks, over a dozen United States banks, including Wells Fargo, Citigroup, JP Morgan Chase, and Bank of America, were hacked between September 2012 and May 2013.[38] Some of these same institutions experienced similar breaches of computer security systems again in 2014.[39]

33. *See* Elizabeth Rowe, *Trade Secrets, Data Security and Employees*, 84 CHI.-KENT L. REV. 749, 750 (2010) (citing recent statistics suggesting that 80% of computer crimes are committed by employees).

34. 18 U.S.C. § 1839 (2012). Trade secret protection is a matter of state law. Many states adopt the Uniform Trade Secrets Act (UTSA). Others have implemented their own legislation. Nevertheless, the core elements of trade secret protection, and a misappropriation cause of action, are functionally equivalent regardless of the exact law adopted by each state.

35. *Id.*

36. The criminals in this attack are believed to be a multinational gang of hackers from Russia, Ukraine, and elsewhere in Europe. *The Great Bank Robbery: Carbanak Cybergang Steals $1bn from 100 Financial Institutions Worldwide*, VIRUS NEWS (Feb. 16, 2015), http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide.

37. David E. Sanger & Nicole Perlroth, *Bank Hackers Steal Millions via Malware*, N.Y. TIMES (Feb. 14, 2015), http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html.

38. Menn, *supra* note 21; McCormick, *supra* note 21.

39. Danny Yadron, Emily Glazer & Devlin Barrett, *FBI Probes Possible Hacking Incident at J.P. Morgan*, WALL ST. J. (Aug. 28, 2015, 8:44 AM), http://www.wsj.com/articles/fbi-probes-possible-computer-hacking-incident-at-j-p-morgan-1409168480.

Banks are acutely susceptible to cybersecurity threats for several reasons. An obvious factor is that banks hold more critical customer information than do retailers. Further, larger financial institutions are constantly acquiring smaller banks. Frequent merger and acquisition activity creates a revolving door of new security systems and access points, thus challenging the acquiring-bank's ability to maintain a coherent, company-wide information security policy.[40] Banks also attract a wider, and perhaps more sophisticated, group of cybercriminals. Many hackers who target financial institutions are interested in causing larger-scale financial disruptions.[41] The victims of these attacks range from shareholders to customers, as well as employees of companies and third-parties with whom the institution relies on for business.

Banks are not the only financial institutions at risk, and a recent uptick in cyber-attacks has generated responses from regulators. In 2014, the SEC Office of Compliance Inspections and Examinations (OCIE) and the Financial Industry Regulatory Authority (FINRA) conducted a sweep of member broker-dealer firms to assess their cybersecurity practices. In 2015, OCIE reported that out of fifty-seven registered broker-dealers and forty-nine investment advisers that were examined, the registered broker-dealers have higher "cybersecurity preparation" than the investment advisers.[42] In 2020, the OCIE revisited these important issues and noted that most firms identified and described cybersecurity roles and responsibilities, required their vendors to also provide their own risk assessments, and had some system to detect and monitor data loss.[43]

However, OCIE noted that there were issues with firms individually tailoring their security policies to their firm and the enforcement of their own policies.[44] Custom-made systems generate problems that are not readily fixable and may be subject to particular risk if there is not an achievable "fix." Moreover, the failure of firms to monitor and enforce their security policies is an age-old problem.

From 2017 through 2019, the OCIE has included cybersecurity as one of its priorities each year. In 2017, the OCIE noted "we will continue our initiative to examine for cybersecurity compliance procedures and controls,

40. Andrea Peterson, *Banks Are Struggling with Cybersecurity. That Doesn't Bode Well for Other Industries*, WASH. POST (Oct. 3, 2014), https://www.washingtonpost.com/blogs/the-switch/wp/2014/10/03/banks-are-struggling-with-cybersecurity-that-doesnt-bode-well-for-other-industries/.

41. *Id.*

42. Samuel Wolff et al., *Cybersecurity and the SEC: Part 2*, *in* 38 SECURITIES AND FEDERAL CORPORATE LAW REPORT 1–2 (Thomson Reuters 2016).

43. U.S. SEC. & EXCH. COMM'N, OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, 2020 EXAMINATION PRIORITIES 13 (2020), https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2020.pdf.

44. *Id.*

including testing the implementation of those procedures and controls."[45] In 2018, the OCIE remarked that "[t]he scope and severity of risks that cyber threats present have increased dramatically."[46] In 2019, the OCIE proclaimed that it was "working with firms to identify and manage cybersecurity risks and to encourage market participants to actively and effectively engage in this effort."[47]

In keeping with its priorities, the OCIE also released a string of "Risk Alerts" between 2017 and 2019. For instance, in August 2017, the SEC issued a Risk Alert regarding companies implementing and addressing sufficient written policies related to the SEC's Cybersecurity Initiative.[48] The SEC found that many of the written policies were generic and not specifically tailored to the individual broker-dealer.[49] The Risk Alert also identified some elements of robust policies: maintenance of an inventory of data, vendor information, detailed cybersecurity-related instructions, and maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities.[50]

In April 2019, the SEC issued a Risk Alert related to Regulation S-P.[51] This Risk Alert involved aiding companies in complying with their obligations under Regulation S-P to provide customers with privacy notices.[52] The most common compliance issues identified by the Risk Alert involved inaccurate privacy and opt-out notices, failures to follow internal policies and procedures, and even absences of policies and procedures altogether.[53] Interestingly, one of the major compliance issues addressed in the Risk Alert was the storage of information on employees' personal devices that did not contain adequate protection for customer information.[54]

45. U.S. SEC. & EXCH. COMM'N, OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATIONS, EXAMINATION PRIORITIES FOR 2017, at 4 (2017), https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf.

46. U.S. SEC. & EXCH. COMM'N, OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATIONS, 2018 NATIONAL EXAM PROGRAM EXAMINATION PRIORITIES 9 (2018), https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf.

47. U.S. SEC. & EXCH. COMM'N, OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATIONS, 2019 NATIONAL EXAM PROGRAM EXAMINATION PRIORITIES 11 (2019), https://www.sec.gov/files/OCIE%202019%20Priorities.pdf.

48. *See generally* U.S. SEC. & EXCH. COMM'N, OBSERVATIONS FROM CYBERSECURITY EXAMINATIONS (Aug. 7, 2017), https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

49. *Id.*

50. *See id.*

51. *See generally* U.S. SEC. & EXCH. COMM'N, OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATIONS, INVESTMENT ADVISER AND BROKER-DEALER COMPLIANCE ISSUES RELATED TO REGULATION S-P—PRIVACY NOTICES AND SAFEGUARD POLICIES (Apr. 16, 2019), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf.

52. *Id.*

53. *Id.*

54. *Id.*

As recently as May 23, 2019, OCIE issued a Risk Alert involving storage of "electronic customer records and information by broker-dealers and investment advisors in various storage solutions."[55] Specifically, OCIE identified that these storage solutions may "raise compliance issues under Regulations S-P and S-ID."[56] The Risk Alert identified that many of the issues surrounding these storage solutions involved firms that failed to configure their security systems to prevent unauthorized access or failed to implement policies to ensure that the security systems were in compliance with their own firm standards.[57]

In 2015, FINRA issued a report outlining its findings.[58] It provided a set of "principles and effective practices" that member firms are recommended to implement. According to the report, firms should:

- "[e]stablish and implement a cybersecurity governance framework that supports informed decision-making and escalation within the organization to identify and manage cybersecurity risks";
- "[c]onduct regular assessments to identify cybersecurity risks associated with firm assets and vendors and prioritize their remediation";
- "[i]mplement technical controls to protect firm software and hardware that stores and processes data, as well as the data itself";
- "[e]stablish policies and procedures, and roles and responsibilities, for escalating and responding to cybersecurity incidents";
- "[m]anage cybersecurity risk that can arise across the lifecycle of vendor relationships using a risk-based approach to vendor management";
- "[p]rovide cybersecurity training that is tailored to staff needs";
- "[u]se cyber threat intelligence to improve capabilities to identify, detect and respond to cybersecurity threat";
- "[e]valuate the utility of cyber insurance as a way to transfer some risk . . ."[59]

55. U.S. SEC. & EXCH. COMM'N, SAFEGUARDING CUSTOMER RECORDS AND INFORMATION IN NETWORK STORAGE–USE OF THIRD PARTY SECURITY FEATURES (May 23, 2019), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf.

56. *Id.*

57. *Id.*

58. FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES 39–41 (Feb. 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf. The quoted language is collected from the "Principles" summaries in Appendix I of the FINRA report, which outline guidance for their respective sections. *See id.*

59. *Id.* at 39–41.

In addition to FINRA's oversight of broker-dealers, banks must comply with the Gramm-Leach-Bliley Act, which imposes an affirmative obligation on banks to guard customers' personal information.[60] Financial institutions must remain vigilant and stay abreast of cutting-edge cybersecurity practices to best ensure they are adequately protected against these growing threats.

2. Public Companies

There have been several recent cyber-attacks against high-profile, public companies.[61] When a public company suffers a cyber-breach, customer information can be compromised, and stockholders may see their share value decline.[62] Still, in the absence of a breach, the very threat of an attack may chill investment in and preempt online purchases from a company perceived to have weak cybersecurity. A study by the Ponemon Institute, which surveyed 507 companies globally, found that the average annual cost of cyber-breaches was $3.92 million.[63] After a breach, businesses also stand to lose reputational capital and other intangible assets, like intellectual property and trade secrets.[64]

The SEC has taken notice of these costs and vowed to play a greater role in regulating companies' internal controls and cyber-related disclosures. Chicago Regional Director David Glockner acknowledged that cybersecurity "is an area where we have not brought a significant number of cases yet," but stated it "is high on our radar screen."[65] Members of Congress agreed and called upon then-SEC Chair Mary Jo White to increase SEC guidance on cybersecurity disclosure.[66]

60. *See* Shields, *supra* note 11, at 357. The Act's substantive provisions are addressed in the sections below.

61. In 2014 alone, Home Depot, JP Morgan Chase, Kmart, Dairy Queen, and Sony Picture Entertainment were each hacked. Noah G. Susskind, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J.L. & BUS. 573, 576–77 (2015). In 2017, Equifax was the victim of a cyber-attack. *See* Josh Fruhlinger, *Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?*, CSO ONLINE (Feb. 12, 2020), https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

62. Susskind, *supra* note 61, at 575.

63. *How Much Would a Data Breach Cost Your Business?*, IBM, https://www.ibm.com/security/data-breach (last visited Apr. 10, 2020).

64. Toni Scott Reed, *Cybercrime: Losses, Claims, and Potential Insurance Coverage for the Technology Hazards of the Twenty-First Century*, 20 FIDELITY L.J. 55, 68 (2014), https://www.fidelitylaw.org/public-pdf/vol_xx/cybercrime.pdf (describing the general effects of cybercrime on businesses and the economy).

65. Sarah N. Lynch, *SEC on the Prowl for Cyber Security Cases: Official*, REUTERS (Feb. 20, 2015, 4:09 PM), http://www.reuters.com/article/2015/02/20/us-sec-cyber-idUSKBN0LO28H20150220.

66. Mark S. Nelson, *Congressmen Ask Chair White to Reboot Cybersecurity Guidance*, WOLTERS KLUWER FIN. SERVICES, US, 1 (June 23, 2015).

The current SEC Chair, Jay Clayton, was specifically questioned about cybersecurity during his confirmation hearings before the Senate.[67] Clayton acknowledged in his confirmation hearings that current cybersecurity disclosures are "currently inconsistent" and that "informed cybersecurity oversight at the board level would be relevant to investors."[68] When Clayton was in private practice prior to joining the SEC, he opined that little was understood about cybersecurity and that companies were still in the early stages of "coming to terms with cybersecurity."[69]

Notably, the SEC went after Facebook following its data breach.[70] After the SEC filed a complaint in 2019, Facebook agreed to pay a $100 million fine to the SEC.[71] This is significant as the Facebook data breach was a debated topic during the 2016 presidential election.

3. Third-Party Vendors and Smaller Companies

Non-public companies, including law and public relations firms, as well as smaller retailers, banks, and credit unions, are also at risk of suffering a cyber-attack. In fact, smaller companies face a greater threat of being hacked than do larger enterprises. A 2012 survey found that 71% of cyber-attacks take place at firms with less than 100 employees.[72] This threat is greatest for companies that serve as intermediaries to large businesses that either store or have temporary access to vast amounts of data. Even if not publicly traded or formally regulated by FINRA or the SEC, these businesses face essentially the same civil liability exposure as do larger companies. Moreover, smaller companies stand to suffer greater damage from a breach because they may lack resources and access to superior cybersecurity safeguards and response teams. Smaller companies must consider similar, but proportional, measures as larger institutions and public companies to guard against cyber-attacks.

C. LEGAL AND REGULATORY EXPOSURE

The failure to adequately prevent a cyber-threat exposes companies to significant civil and regulatory liability. The following sections outline the primary areas of liability facing companies and cyber-thieves.

67. Danielle C. Gray & Patrick D. McKegney, *What to Expect from the SEC's New Cyber-Savvy Chair*, N.Y.L.J. (June 5, 2017, 12:00 AM), https://www.law.com/newyorklawjournal/almID/1202788074707/What-to-Expect-From-the-SECs-New-CyberSavvy-Chair/?slreturn=20190206102815.

68. *Id.*

69. *Id.*

70. Press Release, U.S. Sec. & Exch. Comm'n, Facebook to Pay $100 Million for Misleading Investors About the Risks it Faced from Misuse of User Data (July 24, 2019), https://www.sec.gov/news/press-release/2019-140.

71. *Id.*

72. Lou Shipley, *How Small Businesses Can Fend Off Hackers*, WALL ST. J. (July 16, 2015, 7:09 PM), http://www.wsj.com/articles/how-small-businesses-can-fend-off-hackers-1437088140.

1. Relevant Statutes

a. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA)[73] is the primary statute for prosecuting hacking and other nefarious cyber-activities.[74] Generally, the CFAA prohibits unauthorized access of data from protected computers.[75] "Protected computer" is broadly defined to include computers used by financial institutions, the U.S. Government, and those "used in or affecting interstate or foreign commerce."[76] In 2015, the Second Circuit in *United States v. Valle* noted that this definition of "protected computer" "includes effectively all computers with Internet access."[77] Thus, the CFAA covers a wide swath of entities, including those most often affected by cybercrime.

Apart from unauthorized computer access, the CFAA proscribes several other areas of online criminal conduct. The CFAA prohibits intentional or reckless causation of damage to computer systems, unauthorized access with the intent to defraud, and trafficking in passwords and similar customer information.[78] Violating the CFAA may result in up to ten years imprisonment, fines up to $250,000 (or two times the loss incurred by the victim), and forfeiture or restitution.[79] The CFAA imposes liability for primary actors as well as co-conspirators, and it is interpreted broadly by courts.[80]

However, damages for data piracy under the CFAA are limited by statute and have been interpreted to be limited by court decisions.[81] The U.S. District Court for the Southern District of New York noted that losses under the CFAA are "interpreted narrowly" and only include costs actually related to the damage of a computer system, not the subsequent injuries arising from misappropriated information.[82] The district court observed that the Second

73. 18 U.S.C. § 1030 (2012).

74. *Id.*

75. *Id.*

76. *Id.*

77. United States v. Valle, 807 F.3d 508, 528 (2d. Cir. 2015). Similarly, commentators have suggested, based on state law, that intangible property such as electronic data can be converted and thus constitutes a crime. *See* Richard Raysman & Peter Brown, *Courts Address When an Alleged Employee Hacking is a Crime*, N.Y.L.J. (Aug. 8, 2016) (citing Integrated Direct Marketing v. May, 495 S.W.3d 73 (Ark. 2016)).

78. *See* Philip F. DiSanto, *Blurred Lines of Identity Crimes: Intersection of the First Amendment and Federal Identity Fraud*, 115 COLUM. L. REV. 941, 951–52 (2015) (citing to 18 U.S.C. § 1030(a)(1)–(6)).

79. Ronald W. Breaux et al., *A Guide to Data Protection and Breach Response – Part 2*, 26 INTELL. PROP. & TECH. L.J. 23, 23–24 (2014).

80. DiSanto, *supra* note 78, at 952.

81. Shari Lewis, *Asserting Damages for Data Piracy Under the CFAA*, LAW.COM (June 19, 2017, 2:03 PM), https://www.law.com/newyorklawjournal/sites/newyorklawjournal/2017/06/19/asserting-damages-for-data-piracy-under-the-cfaa/?slreturn=20200024174900.

82. *See* Reis v. Lennar, No. 15 Civ. 7905, 2016 WL 3702736, at *5 (GBD) (S.D.N.Y. July 5, 2016).

Circuit had already opined on the issue and noted that the damages, under the CFAA, are truly limited to the effects of repairing damage as a result of a prior intrusion and do not include money expended on improving system integrity following a data breach.[83] An example of damages that would be recoverable under the CFAA are money expended to repair a server following a security breach.[84]

b. Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) governs the unauthorized interception of online communications and includes three titles: (1) the Wiretap Act, (2) the Stored Communications Act (SCA), and (3) the Pen Registry Act.[85]

The Wiretap Act proscribes wiretapping, or the interception of wire, oral, or electronic communications.[86] The SCA prohibits unauthorized access to stored electronic communications and communications transactions records.[87] A violation of the SCA may result in a fine or imprisonment of up to ten years. The SCA, as well as the Wiretap Act, allows service providers to access or disclose stored communications under certain exemptions to protect the rights or property of the provider.[88] In addition, the SCA authorizes service providers to inform law enforcement of the contents of customer communications if the data is "inadvertently obtained by the service provider" and "appear[s] to pertain to the commission of a crime."[89] However, critics argue that these provisions are vaguely drafted and as a result, inadequately protect providers from making good faith attempts to notify authorities of potential threats, absent express statutory authorization.[90] Finally, the Pen Registry Act makes it illegal to use trap and trace devices and pen registers, which are devices that monitor and record numbers dialed—or messages sent—to and from a particular device.[91]

Some argue that the ECPA's protections hinder critical information sharing by service providers for fear of violating the ECPA's privacy provisions.[92] Importantly, however, the ECPA contains a number of key exemptions. Under the Wiretap Act, communications service providers, such as telecommunications companies, may intercept protected communications

83. Lewis, *supra* note 81.
84. *Id.*
85. 18 U.S.C. §§ 2510–2522 (2012); 18 U.S.C. §§ 2701–2712; 18 U.S.C. §§ 3121–3127.
86. 18 U.S.C. §§ 2510–2522.
87. *Id.* at §§ 2701–2712.
88. *Id.* at § 2702(b)(5).
89. *Id.* at § 2702(b)(7).
90. Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor,"* 18 VA. J.L. & TECH. 289, 321 (2014).
91. 18 U.S.C. §§ 3121, 3127 (2012).
92. *See, e.g.*, Palmer, *supra* note 90, at 320–321 (arguing that the ECPA's provisions function as barriers to information sharing about cyber-attacks).

if doing so is incidental to "the rendition of service or the protection of the rights or the property of the provider," or to guard against fraud.[93] Service providers must receive a court order, however, before they can share information about a cyber-threat with law enforcement.[94] Thus, where the service provider is not the victim of an attack, the ECPA potentially "hinder[s] sharing of information about cyber threats."[95]

c. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act[96] (GLBA) is aimed at thwarting cyber-attacks within the financial services industry. The GLBA expressly and exclusively applies to financial institutions, defined as: "any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution," amongst others.[97]

The Act authorizes federal agencies, including the Federal Trade Commission (FTC) and Federal Deposit Insurance Corporation (FDIC), to issue regulations governing the data security systems of covered institutions.[98] For example, pursuant to the GLBA, the Federal Reserve Board issued guidance requiring covered banks to report to its board at least annually as to "the overall status" of its information security systems.[99]

Title V of the GLBA places an affirmative duty on financial institutions to "protect the security and confidentiality" of customers' personal information.[100] To further this end, companies covered by the GLBA must establish comprehensive standards relating to administrative, technical, and physical safeguards.[101] These safeguards must: (1) insure the security and confidentiality of customer information; (2) protect against anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[102]

The GLBA does not outline specific penalties for violating these provisions. Rather, it authorizes enforcement agencies, such as the FTC, to charge the institutions for violations.[103] Penalties range from monetary

93. 18 U.S.C. §2511(2)(a)(i), (h)(ii).

94. Casey M. Bruner, *Authorized Investigation: A Temperate Alternative to Cyber Insecurity*, 38 SEATTLE U. L. REV. 1463, 1470 (2015).

95. EDWARD C. LIU ET AL., CONG. RESEARCH SERV., R42409, CYBERSECURITY: SELECTED LEGAL ISSUES 22 (2013), https://www.fas.org/sgp/crs/misc/R42409.pdf.

96. 15 U.S.C. § 6801 (1999).

97. *Id.* at § 6827(4).

98. Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1537–38 (2013).

99. 12 C.F.R. pt. 225, App. F (III)(F) (2013).

100. 15 U.S.C. § 6801(a).

101. *Id.* at § 6801(b).

102. *Id.*

103. Sales, *supra* note 98, at 1538.

sanctions to sheer reputational damage that accompanies an agency bringing a case against a member institution.[104] Financial services firms have made large investments in information security systems since the GLBA's passage.[105] As a result, the GLBA is an example of how implementing federal standards—accompanied by the threat of civil liability for non-compliance—can promote better cybersecurity procedures.[106]

d. Economic Espionage Act

The Economic Espionage Act (EEA)[107] criminalizes economic espionage and trade secret theft. It defines the former as "theft for the benefit of a foreign entity" and the latter as stealing trade secrets for "pecuniary gain."[108] Despite distinguishing between these two types of crimes, the EEA maintains a singular definition of "misappropriation." The EEA imposes liability on any individual or entity that: (1) steals, or appropriates a trade secret without authorization, or by fraud; (2) copies, downloads, or otherwise alters a trade secret without authorization; or (3) knowingly buys, receives, or possesses a stolen trade secret.[109] The term "trade secret" is defined broadly to include almost any intellectual property owned by a business.[110] Violating the EEA may result in up to fifteen years imprisonment as well as fines up to $5 million for an individual and up to $10 million ("or three times the value of stolen trade secret to that organization") for an organization.[111] The EEA, as with the CFAA, holds co-conspirators liable for their role in committing misappropriation.[112]

Until recently, "trade secrets were only protected by: (i) state law; (ii) criminal prosecution under the [EEA] . . . ."[113] The Defend Trade Secrets Act of 2016 (DTSA),[114] adds a civil remedy to the EEA. The DTSA does preempt state law, but it is rather intended to co-exist with state law. The DTSA provides companies with the *ex parte* civil seizure remedy to prevent misappropriation of trade secrets.[115] Under the DTSA, companies may now

104. *Id.*

105. *Id.* (citing Benjamin Powell, *Is Cybersecurity a Public Good? Evidence from the Financial Services Industry*, 1 J.L. ECON. & POL'Y 497, 502 (2005)).

106. *Id.* at 1539.

107. 18 U.S.C. §§ 1831–1839 (2012).

108. *See* Gavin C. Reid et al., *What's it Worth to Keep a Secret?*, 13 DUKE L. & TECH. REV. 116, 131–32 (2015).

109. Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317, 332–33 (2015).

110. *See* 18 U.S.C. § 1839.

111. Joseph Fazioli & Mauricio A. Espana, *Economic Espionage and Trade Secrets Enforcement Under the Trump Administration*, N.Y.L.J., Jan. 30, 2017, at S2.

112. Seaman, *supra* note 109, at 333.

113. Howard Wintner, *Civil Seizure Remedies Under the Defend Trade Secrets Act*, N.Y.L.J., May 11, 2016, at 4, 9.

114. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376.

115. Lawrence Elbaum, *Issues for Companies Under New Trade Secrets Law*, N.Y.L.J., June 17, 2016, at 4.

bring lawsuits for misappropriation of trade secrets in federal court.[116] In addition, under the DTSA, employees who want to report suspected violations of law are granted "immunity from liability for disclosing trade secret material to the government, an attorney, or in a court filing made under seal."[117]

For example, last year, federal prosecutors, among other things, filed charges under EEA against Huawei Technologies Co., "China's largest technology company, alleging it stole trade secrets from an American rival and committed bank fraud by violating sanctions against doing business with Iran."[118] This indictment[119] represents the latest in not only tension between the two governments but also the very real threat that cybersecurity represents to companies and their trade secrets. This case should be closely followed as it progresses because this action, if successful, could be used as a basis for actions against other foreign companies doing business in the United States.

e. Cybersecurity Disclosure Act of 2017 and 2018

A bipartisan bill was introduced in the House of Representatives and the Senate in 2017 related to cybersecurity disclosure.[120] The bill tasks the SEC with creating rules related to public companies' disclosures regarding cybersecurity.[121]

f. State Notification Statutes

Currently, all fifty states have data breach notification statutes.[122] These laws typically require an entity that has suffered a breach to notify affected customers when their unencrypted personal information is compromised. The state's attorney general may then pursue lawsuits against companies that fail to provide such notification. Within this general framework, however, the particulars of these laws can differ significantly from state to state.[123]

116. *See id.*

117. *Id.*

118. Patricia Hurtado & Chris Strohm, *U.S. Charges Huawei with Stealing Trade Secrets, Bank Fraud*, BLOOMBERG (Jan. 28, 2019), https://www.bloomberg.com/news/articles/2019-01-28/u-s-planning-to-announce-criminal-charges-related-to-huawei-jrgrda0q.

119. Indictment, United States v. Huawei Co., Ltd., No. CR19-010-RSM (D. Wash. Jan. 16, 2019), *available at* https://www.justice.gov/opa/press-release/file/1124996/download.

120. Cybersecurity Disclosure Act, S. 536, 115th Cong. (2017).

121. *See id.*

122. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Mar. 8, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

123. *See, e.g.*, Christopher J. Cox et al., *Fixing the Patchwork: Will Congress Enact a Federal Data Breach Law?*, *in* 32 WESTLAW J. COMPUTER & INTERNET 2 (June 5, 2015) (describing the wide variation among state notification laws).

A key point of difference between state notification laws is in the definition of "personal information."[124] States vary as to how significant the breach must be to require notification. Another area where these notification laws diverge is in the timeframe within which entities must inform their customers following a cyber-attack.[125] Moreover, only some of these states maintain laws that expressly authorize a private right of action in addition to a lawsuit from the state's attorney general.[126] These distinctions can make compliance with state notification laws difficult for companies that have just suffered a data breach. Accordingly, many are calling for a federal statute that establishes a uniform notification standard.[127]

2. Common Law Claims

Companies that suffer breaches may be sued by customers and other harmed parties in individual or class actions lawsuits. These claims are usually brought under common law causes of action, such as negligence or breach of contract. They may also be pursued under relevant state statutes, such as consumer protection or notification laws.

a. Class Action Issues

When a company suffers a data breach, customers will often pursue their claims collectively as a class action. Before addressing the legal claims that plaintiffs pursue in such actions, threshold issues related to standing and certification should be addressed.

To have standing to sue in federal court, the plaintiff must suffer an injury that is traceable to the defendant's conduct and capable of redress by a favorable decision.[128] As discussed more fully below, most data breach plaintiffs struggle to establish a legally cognizable injury. Generally, class actions fail when prospective customer class members have no tangible injury but instead class members allege speculative harm, such as risk of future misappropriation or breach.[129] The injury in fact requirement is readily met, however, if the plaintiffs can show that the breach resulted in direct financial harm to the class members.[130]

124. Rachael M. Peters, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1182 (2014).

125. Only a handful of states prescribe a specific time frame, which can range from five days to forty-five days. *Id.*; *see also* Cox et al., *supra* note 123, at 2 ("One of the most widely cited points of divergence among state data breach laws is the timing of notification.").

126. Shields, *supra* note 11, at 356.

127. *Bloomberg: Obama Revives Consumer Privacy and Security Proposals*, CDT (Jan. 16, 2015), https://cdt.org/press/bloomberg-obama-revives-consumer-privacy-and-security-proposals/.

128. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

129. Angelo A. Stio III et al., *Standing and the Emerging Law of Data Breach Class Actions*, 293 N.J. LAW. 70 (2015).

130. *See* Cease, *supra* note 6, at 399.

If standing is established, the prospective class must still meet class certification requirements under federal procedural rules. The first step is satisfying Rule 23(a), which has four prerequisites: (1) numerosity; (2) commonality; (3) typicality; and (4) adequacy of representation.[131] Generally, plaintiffs that survive the standing inquiry will meet these preliminary requirements;[132] the real battle is waged on Rule 23(b)(3).

Every class seeking damages rather than injunctive relief must meet the predominance requirement. Specifically, under Rule 23(b)(3), they must show that "questions of law or fact common to class members predominate over any questions affecting only individual members."[133] Data breach plaintiffs struggle to meet this requirement when individualized damages vary across members of the class.[134] The class will not be certified when individual issues as to the plaintiffs overwhelm common questions regarding the breach or the defendant's conduct in failing to prevent the cyber-attack. Similarly, predominance will not be met when other issues, such as proving liability, differ among class members.[135] Thus, the large, complex, and individualized nature of harm in a typical data breach works against the plaintiffs' favor in data breach class actions.

Despite these procedural hurdles, "plaintiffs have filed nine federal class action securities fraud lawsuits against public companies after data security incidents."[136] These lawsuits come in the wake of major cyber-incidents involving companies such as Yahoo! and Equifax, ironically a company tasked with protecting people's personally identifiable information.[137] The plaintiffs in the Equifax lawsuit[138] alleged, in sum and substance, that the company overstated its security procedure; therefore, the alleged overstatements rendered the company's disclosures misleading.[139] The company had recently disclosed in its public financial statements for 2015 and 2016 that it had developed "new technology to enhance . . . the security of the services [it] offer[s]."[140]

In two other class actions, plaintiffs alleged, despite general acknowledgment of cybersecurity risks in periodic disclosures, companies

131. *See* FED. R. CIV. P. 23(a).

132. *See* Cease, *supra* note 6, at 414.

133. FED. R. CIV. P. 23(b)(3).

134. *See* J. Thomas Richie, *Data Breach Class Actions*, 44 BRIEF 12, 16 (2015).

135. *See* Cease, *supra* note 6, at 417–19 (describing, as a difficulty in meeting the predominance inquiry, that "'different states' laws may apply to different individuals within the class").

136. Derek Borchardt & Craig A. Newman, *The Next Big Thing: Data Breach Securities Class Action Litigation*, PATTERSON BELKNAP WEBB & TYLER LLP (Feb. 20, 2018), https://www.pbwt.com/data-security-law-blog/the-next-big-thing-data-breach-securities-class-action-litigation.

137. *See id.*

138. *See* Class Action Complaint for the Violation of the Federal Securities Laws, Kuhns v. Equifax Inc., 17-cv-03463 (N.D. Ga. Sept. 8, 2017).

139. *See* Borchardt & Newman, *supra* note 136.

140. *Id.*

failed to disclose more specific security risks, and their stock price was artificially inflated as a result.[141] These cases, filed against Intel Corp. and Advanced Micro Devices, Inc., raise significant questions as to the specificity of companies' disclosures.

b. Negligence

When an individual's information is compromised in a data breach, he or she may pursue a negligence action against the entity that housed the data. A common law negligence claim has four elements: (1) duty, (2) breach, (3) causation, and (4) damages or injury.[142] Typically, a data breach plaintiff will allege one or both of the following: the business was negligent in protecting the information or in failing to timely notify harmed parties. If the plaintiff can demonstrate the defendant had a duty to protect the information, the first three elements can readily be satisfied.[143] However, data breach plaintiffs have had difficulty with the injury requirement.[144]

A tangible, non-speculative injury is crucial to a successful negligence claim.[145] In the strongest claim, the plaintiff has been directly harmed. For instance, when personally identifiable information was stolen and may be used to withdraw money from the plaintiff's bank account or to conduct fraudulent transactions.[146] The middle ground lies in cases where, although customer information was accessed, no unauthorized purchases or transactions were initiated.[147] In these cases, plaintiffs will argue that other injuries were incurred, such as cancelling the credit card, waiting to receive a new one, credit monitoring fees, and the loss of reward points.[148] Plaintiffs might also assert loss of privacy and emotional injury, though such claims have not been well received by courts.[149] Finally, the plaintiff may allege that, although no unauthorized access has occurred, the defendant inadequately protects information; therefore, the defendant is susceptible to a breach in the imminent future.[150] This last category is the weakest claim. Courts have, unsurprisingly, held that increased risk of future harm is insufficient to state a cognizable legal injury.[151]

---

141. *See id.*

142. *See* Norman Siegel et al., *Securing Data-Breach Claims*, 51 TRIAL 22, 26 (2015).

143. *Id.*

144. *Id.*

145. *See* Douglas H. Meal, *Private Data Security Breach Litigation in the United States*, ASPATORE (Jan. 2014), 2014 WL 10442, at *2 (observing that "absent allegations of actual, detrimental misuse of their information, plaintiffs have had great difficulty establishing any injury sufficient to support their claims.").

146. *See* Cease, *supra* note 6, at 398.

147. *See id.* at 399.

148. *Id.*

149. *See* Meal, *supra* note 145, at *3.

150. Cease, *supra* note 6, at 404.

151. Meal, *supra* note 145; *see also* James DeGraw, Seth Harrington & David T. Cohen, *Practical Tips for In-House Counsel from Recent Private Data Security Breach Litigation*, BLOOMBERG L.

c. Breach of Contract

Following a cyber-attack, a plaintiff-customer may also attempt to bring a breach of contract claim. While contract law varies state-by-state, a breach of contract claim generally requires the plaintiff to prove four elements: (1) an enforceable agreement, (2) fulfillment of obligations by the non-breaching party, (3) failure to fulfill by the breaching party, and (4) damages to the non-breaching party resulting from the breach.[152] In most cases, data breach plaintiffs will have difficulty meeting the threshold showing of a contractual relationship between the customer and the named defendant.[153] Moreover, an express agreement where the attacked company promises to safeguard the plaintiff's information is often missing.[154]

Without an express agreement, plaintiffs may seek to hold the company liable under a theory of breach of an implied contract. The elements of this claim are identical to a traditional breach of contract action except for the requirement of an express agreement. Instead, the parties' mutual assent is objectively viewed through their conduct rather than words.[155] In these cases, the customer will argue that the merchant implicitly agreed to safeguard their information when the data was provided because it was given with the purpose of being held exclusively by the merchant; it was not given with the expectation that unauthorized third-parties would access it.[156] This rationale was accepted in *Target*, where the court allowed the plaintiffs' breach of implied contract claim to survive a motion to dismiss.[157] Courts will, however, generally dismiss such claims absent proof of a direct relationship between the plaintiff and the breached company.[158] Moreover, assuming a contract does exist, implied or express, plaintiffs will still have to prove damages. As with negligence claims, plaintiffs may face the same difficulties in showing they suffered legally cognizable harm as a result of the breach.

(Sept. 28, 2016), https://news.bloomberglaw.com/health-law-and-business/practical-tips-for-in-house-counsel-from-recent-private-data-security-breach-litigation (examining recent cases which show that, at the motion to dismiss stage, courts may take into consideration companies' public statements to determine "whether a sufficient injury exists").

152. *See, e.g.*, Fischer & Mandell, LLP v. Citibank, N.A., 632 F.3d 793, 799 (2d Cir. 2011); Kaloe Shipping Co. v. Goltens Service Co., 315 F. App'x 877, 880 (11th Cir. 2009).

153. Jonathan J. Darrow & Stephen D. Lichtenstein, *"Do You Really Need My Social Security Number?" Data Collection Practices in the Digital Age*, 10 N.C.J.L. & TECH. 1, 28 (2008) ("[M]any organizations that possess sensitive personal data do not have contractual relationships with consumers at all, since they have obtained the information elsewhere.").

154. Courts also decline to find company statements and policies about security practices enforceable. Meal, *supra* note 145, at *5.

155. *Id.*

156. *See* Anderson v. Hannaford Bros., 659 F.3d 151, 159 (1st Cir. 2011) ("When a customer uses a credit card in a commercial transaction, she intends to provide that data for the merchant only . . . . A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract.").

157. *In re* Target Corp. Data Sec. Breach Litigation, 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014).

158. Meal, *supra* note 145, at *5.

3. Derivative Shareholder Suits

Publicly traded companies that suffer a decline in share value after a cyber-attack face the threat of a derivative suit. In a derivative action, shareholders are permitted to bring a suit on the corporation's behalf for wrongful acts that deplete corporate assets or cause other harm to the entity.[159]

In a data breach derivative claim, shareholders may assert that officers or directors inadequately managed the response to an attack.[160] Recently, Wyndham Worldwide Corporation shareholders filed a derivate action against the hotel and resort giant. The shareholders alleged, albeit unsuccessfully, that the board failed to adequately protect customer information after a breach, thereby causing harm to the company.[161]

Shareholders may also allege that the company misrepresented its risk or the existence of an attack, or failed to disclose infirmities in its control systems.[162] In early 2014, a derivative action was brought against Target's board of directors.[163] The shareholders alleged that Target failed to take adequate steps to prevent the attack, and the company provided misleading information to customers as to the extent of the harm in its wake.[164] As the prevalence of data breaches and the sophistication of hackers increases, the threat of derivative suit liability increases as well. Boards need to allocate time and resources commensurate with these growing threats to ensure cybersecurity controls are consistent with industry standards.

4. SEC Regulations and Disclosure Issues

The SEC's efforts within the cybersecurity realm focus on achieving two general aims: protecting investor data and ensuring disclosure of material information related to cyber-risks and data breaches.[165] The Commission has issued a number of specific rules to further these goals.

159. *See* Kemen v. Kemper Fin. Servs., Inc., 111 S. Ct. 1711, 1716 (1991).

160. Jay A. Dubow & Pamela S. Palmer, *Key Challenges and Concerns for Securities Law Defense Attorneys*, ASPATORE (Apr. 2015), 2015 WL 2407609, at *3.

161. The court eventually dismissed these claims. Palkon v. Holmes, No. 14-cv-01234, 2014 WL 5341880, at *1, *7 (D. N.J. Oct. 20, 2014).

162. Dubow & Palmer, *supra* note 160, at *3.

163. Craig A. Newman, *Target Corp. Shareholders Walk Away from Derivative Lawsuits*, PATTERSON BELKNAP WEBB & TYLER LLP (July 8, 2016), https://www.pbwt.com/data-security-law-blog/target-corp-shareholders-walk-away-derivative-lawsuits.

164. Jamie Santo, *Target Execs Slapped with Investor Suit over Data Breach*, LAW 360 (Jan. 29, 2014, 10:53 PM), http://www.law360.com/articles/505257/target-execs-slapped-with-investor-suit-over-data-breach.

165. Lisa J. Sotto et al., *SEC Cybersecurity Investigations: A How-To Guide*, 21 WESTLAW J. SEC. LITIG. & REG. 1 (2015).

a. Regulation Systems Compliance and Integrity

The SEC adopted Regulation Systems Compliance and Integrity (SCI) in November 2014.[166] Regulation SCI applies to self-regulatory organizations, certain alternative trading systems, plan processors, and exempt clearing agencies subject to the Commission's Automation Review Policy statements.[167] The purpose of the regulation is to strengthen the infrastructure of the securities markets with the hope of preventing market disruptions that result from technological failures.[168]

Regulation SCI requires covered entities to implement policies and procedures regarding their trading, clearance, order routing, market data, regulation, and surveillance systems.[169] Securities exchanges must also maintain and test backup systems and disaster recovery plans.[170] In addition, Regulation SCI mandates that these entities conduct annual reviews and quarterly reports, maintain books and records, and provide notification and updates to the SEC as to systems vulnerabilities.[171]

On July 8, 2015, trading was halted on the New York Stock Exchange (NYSE) for around three hours, purportedly due to a software glitch.[172] The jury is still out on if Regulation SCI has mitigated the risk of future market disruptions. We are uncertain as to the efficacy of Regulation SCI's effect and if it will mitigate the effect of future market disruptions.

b. Regulation S-ID

Regulation S-ID is aimed at preventing identity theft and applies to most broker-dealers, mutual funds, and investment advisers.[173] It requires these entities to develop programs and procedures to detect red flags and "prevent and mitigate identity theft."[174] Entities must also obtain board approval,

166. Press Release, U.S. Sec. & Exch. Comm'n, SEC Adopts Rules to Improve Systems Compliance and Integrity: Rules to Strengthen Technology Infrastructure of Securities Markets (Nov. 19, 2014), https://www.sec.gov/news/press-release/2014-260.

167. Regulation Systems Compliance and Integrity, Exchange Act Release No. 73639, 2014 WL 6850916, at *1 (Nov. 19, 2014).

168. U.S. SEC. & EXCH. COMM'N, SPOTLIGHT ON REGULATION SCI (Dec. 9, 2016), https://www.sec.gov/spotlight/regulation-sci.shtml.

169. Regulation Systems Compliance and Integrity, Exchange Act Release No. 73639, 2014 WL 6850916, at *30 (Nov. 19, 2014).

170. *Id.* at *59.

171. *See* Stephen M. Flanagan, *New Rules to Strengthen Technology Infrastructure of Securities Markets*, 33 FLETCHER CORP. L. ADVISER 11 (2015).

172. Drew Harwell, Thad Moore & Jacob Bogage, *NYSE Resumes Trading After Unprecedented Shutdown*, WASH. POST (July 8, 2015), https://www.washingtonpost.com/business/economy/nyse-trading-has-been-halted/2015/07/08/46b51974-2588-11e5-b72c-2b7d516e1e0e_story.html.

173. Regulation S-ID applies to entities that fall within the definition of "financial institution" and "creditor" under the Fair Credit Reporting Act. Identity Theft Red Flags Rules, 78 Fed. Reg. 23638, 23640–41 (Apr. 19, 2013) (to be codified at 17 C.F.R. pt. 248).

174. *Id.* at 23647.

delegate senior level management oversight, and implement adequate training and updating for identity theft prevention programs.[175]

c. Regulation S-P

Regulation S-P is designed to safeguard customer information and applies to all broker-dealers, investment companies, and investment advisers registered with the SEC.[176] Generally, it requires covered entities to implement written policies and procedures reasonably designed to: (1) insure the security of customer records and information, (2) protect against anticipated threats to the security or integrity of such records and information, and (3) protect against unauthorized access to or use of customer records and information that could result in substantial harm or inconvenience to any customer.[177] Companies must provide "clear and conspicuous" notice adequately describing privacy policies to customers.[178] Entities covered under S-P must also withhold disclosure of non-public customer information to unaffiliated third-parties.[179]

In 2008, concerns mounted that some firms were not regularly reevaluating and updating these safeguards. The SEC then proposed amending Regulation S-P to "set forth more specific requirements for safeguarding information and responding to information security breaches."[180] While the amendment was ultimately shelved, companies should regularly assess and reevaluate their cyber-risks and compliance with Regulation S-P. Failure to adequately protect customer information can lead to an enforcement action and substantial fines.[181]

d. General Disclosure Provisions Related to Cybersecurity Risks & Attacks

In 2011, the SEC issued guidance regarding how companies may address cybersecurity risks, threats, and incidents under existing disclosure items.[182] These guidelines focused on disclosure of: (1) risk factors, (2) management's discussion and analysis (MD&A) of financial condition and results of

175. Brice Kindred, *An Uneasy Balance: Personal Information and Crowdfunding Under the JOBS Act*, 21 RICH. J.L. & TECH. 4, 52 (2015).

176. 17 C.F.R. § 248.30 (2014).

177. *Id.* at § 248.30(a).

178. *Id.* at § 248.4(a).

179. *Id.* at § 248.10.

180. Proposed Amendment to Regulation S-P, Release No. 34-57427, at 1 (proposed Mar. 4, 2008), http://www.sec.gov/rules/proposed/2008/34-57427.pdf.

181. *See* Francoise Gilbert, *SEC Fines Broker-Dealer $275,000 for Failure to Safeguard Customer Information*, 28 BANKING & FIN. SERV. POL'Y REP. 7 (2009).

182. U.S. SEC. & EXCH. COMM'N, DIV. OF CORP. FIN., CF DISCLOSURE GUIDANCE: TOPIC NO. 2 (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [hereinafter CF DISCLOSURE GUIDANCE].

operations, (3) description of business, (4) legal proceedings, (5) financial statement disclosures, and (6) disclosure controls and procedures.[183]

Regarding risk factors, under item 503(c) of Regulation S-K, companies must describe the nature of material risks faced as well as how the entity is affected by those risks. According to the SEC, 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."[184]

Several factors must also be considered when determining if a cyber-risk is material and therefore merits disclosure. Companies should look at the probability of suffering a cyber-incident and both the quantitative and qualitative magnitude of the harm, or risk of harm, that would result from the incident. The quantitative magnitude is measured mainly in terms of financial harm, while the qualitative component accounts for intangibles such as the harm to a company's reputation and good will. Risks include misappropriation of assets or sensitive information, corruption of data, and prolonged disruption of operations.[185] Disclosure as to the scope of cybersecurity insurance coverage is also recommended.[186] Generic and boilerplate disclosure of risk factors should be avoided. Importantly, however, the SEC noted that companies should avoid overly detailed disclosures that could compromise a registrant's cybersecurity.[187]

The SEC has yet to issue any more specific disclosure guidance for cyber-risks and incidents. Also, the SEC has maintained that materiality is the "touchstone" for disclosure to investors.[188] According to a 2016 Audit Analytics study, "only 95 of the approximately 9,000 publicly traded companies have informed the SEC of a data breach since January 2010."[189] To date, the SEC has not brought an enforcement action against a publicly traded company for failure to disclose cybersecurity risks and incidents.[190]

Furthermore, the SEC advises registrants to address cybersecurity risks and incidents in its MD&A disclosures "if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition."[191] The SEC provides an example of when such

183. *See id.*
184. *Id.*
185. *Id.*
186. *Id.*
187. *Id.*
188. Danielle C. Gray & Patrick D. McKegney, *What to Expect From the SEC's New Cyber-Savvy Chair*, N.Y.L.J. (June 5, 2017), https://www.law.com/newyorklawjournal/almID/1202788074707/What-to-Expect-From-the-SECs-New-CyberSavvy-Chair/?slreturn=20190206 10281.
189. *Id.*
190. *Id.*
191. CF DISCLOSURE GUIDANCE, *supra* note 182 (citing Item 303 of Regulation S-K; and Form 20-F, Item 5).

disclosure is warranted and cites theft of intellectual property that is reasonably likely to result in material effects to the company's financial condition.[192]

Item 101 of Regulation S-K governs "Description of Business" disclosures, and it requires disclosures relating to the general development of the registrant's business.[193] Pursuant to the SEC's cybersecurity guidelines, companies should disclose cyber-incidents in this section if one or more incidents "materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions."[194]

Item 103 of Regulation S-K requires disclosure of "material pending legal proceedings, *other than* ordinary routine litigation incidental to the business."[195] The SEC advises companies to disclose material pending litigation involving a cyber-incident to where it or its subsidiary is a party.[196] Companies should follow the rule of advice provided in Item 103, which exempts disclosure of any litigation involving, primarily, a claim for damages when the amount involved is less than 10% of the company's current assets.[197]

Regarding financial statement disclosure, the SEC recognizes the broad impact cyber-attacks have on a company's financial statements before, during, and after an incident. The SEC guidelines advise companies to disclose expenditures related to cyber-issues depending on the nature and severity of the potential or actual incident. For example, companies might need to compensate warranty claimants or incur losses resulting from product recall and replacement after a breach. The SEC suggests that companies make these disclosures if losses are probable and reasonably estimable, or at least reasonably possible.[198] Such disclosures should be made in accordance with existing accounting guidelines and principles companies follow when making such disclosures.[199]

Item 307 of Regulation S-K requires disclosure as to the effectiveness of the company's disclosure controls and procedures.[200] The SEC advises that companies disclose cyber-issues to the extent that they "pose a risk to the registrant's ability to record, process, summarize, and report information that is required to be disclosed in Commission filings."[201] Companies should

192. In the event that the attack does not result in the loss of intellectual property, but, nonetheless, prompts the registrant to materially increase safeguarding expenses, the SEC advises the registrant to note those increased expenditures. *See id.*

193. 17 C.F.R. § 229.101 (2018).

194. CF DISCLOSURE GUIDANCE, *supra* note 182.

195. 17 C.F.R. § 229.103 (2014) (emphasis added).

196. CF DISCLOSURE GUIDANCE, *supra* note 182.

197. 17 C.F.R. § 229.103 (2014).

198. *Id.*

199. *Id.*

200. *See id*. at § 229.307.

201. CF DISCLOSURE GUIDANCE, *supra* note 182.

consider any deficiencies in their disclosure controls that would render reporting ineffective in the event of a cyber-incident. For instance, if it is reasonably possible that a cyber-attack would render information recording improper, then a registrant may conclude that its disclosure controls are ineffective.[202]

II. STRATEGIES AND SOLUTIONS

The following sections recommend security strategies that companies may implement to navigate the current cyber-threat landscape. Section A addresses the preventative steps a board of directors can implement before a breach happens. The board of directors should focus on thoroughly reviewing company procedures and resources, establishing an action plan, and delegating staff responsibilities. Section B describes the immediate action steps companies should consider upon discovering a cyber-attack. Section B also addresses responses to longer-term concerns, such as compliance with legal, regulatory, fiduciary, and public relations obligations, as well as using a breach to improve company preparedness in the future.

A. BEFORE THE BREACH: PREVENTATIVE STEPS

1. The Boardroom: Setting the Tone for Company-Wide and Cross-Departmental Preparedness

Corporate boards must assume the lead in establishing company-wide cybersecurity prevention and response strategies.[203] In June 2014, a speech at the NYSE given by then SEC Commissioner Luis Aguilar appropriately stated, "ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities."[204]

Boards face ample incentivizes to put cybersecurity management front and center. When a businesses' IT systems are breached, it may face costly operational disruptions, substantial response expenses, negative publicity, and reputational damage.[205] The threat of litigation from harmed parties, potentially including state and federal agencies, also looms large. As recent history indicates, directors may be held legally accountable in derivative

202. *Id.*

203. Companies should be mindful of state cybersecurity regulations. For example, the New York State Department of Financial Services (DFS) adopted cyber security regulations, effective January 1, 2017, "which require regulated financial companies doing business in New York to adopt comprehensive written programmes and procedures to prevent data breaches and other cyber security events." Barry R. Temkin & Robert Usinger, *New Cyber Security Regulations Promulgated by New York's Department of Financial Services*, CORP. DISPS.' MAG., Jan.–Mar. 2017, at 2.

204. Luis Aguilar, Comm'r, U.S. Sec. & Exch. Comm'n, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (June 10, 2014), https://www.sec.gov/news/speech/2014-spch061014laa.

205. *Id.*

actions as well.[206] Given the current cyber-threat environment, prudent directors would be hard-pressed to find a compelling justification to ignore proper cyber-risk management. Moreover, boards presently assume similar oversight responsibilities in the realm of credit, liquidity, and operational threats facing the company.[207] Cyber-attacks pose as significant a threat as these existing risk areas must be a part of the board's overall oversight duties going forward.

In his remarks, Commissioner Aguilar suggested key steps boards should take to mitigate exposure to crippling cyber-attacks and improve company responses.[208] The initial steps involve inventory and review. Directors must self-examine current safeguards, expenses, and delegation of responsibility related to IT security programs. Boards should begin by looking to the Framework for Improving Critical Infrastructure Cybersecurity ("the Framework"), issued by the National Institute of Standards and Technology in 2014, for guidance.[209] Aguilar deemed the Framework "a baseline for best practices," and he noted that it provides a rubric against which boards can assess existing practices and any potential deviations that could lead to legal or regulatory exposure.[210]

After reviewing existing practices and resources, the board must work to ensure the company is staffed with the right personnel to carry out its cybersecurity programs. Directors who understand IT and cyber-issues are assets. Currently, 14% of corporate directors across industries say they have a "high level" of cybersecurity-related knowledge.[211] In the absence of director expertise, boards should, at the least, have a clear understanding of which employees it can rely on as sounding boards for cyber-policies. Boards should consider carving out a senior management position devoted to cybersecurity.[212] Without question, the board must also ensure that the IT department devotes full-time personnel to cyber-issues. If the board finds that the company lacks sufficient IT and data security expertise, then it must immediately hire competent personnel. Smaller companies might find it more

206. *See* Kevin M. LaCroix, *Target Corporation Cybersecurity-Related Derivative Litigation Dismissed*, D&O DIARY (July 9, 2016), https://www.dandodiary.com/2016/07/articles/cyber-liability/target-corporation-cybersecurity-related-derivative-litigation-dismissed/.

207. Boards must disclose involvement in the oversight of company risk management in the wake of these material risks. *See* Proxy Disclosure Enhancements, Securities Act Release No. 9089, Exchange Act Release No. 61175, Investment Company Act Release No. 29092, 74 Fed. Reg. 68334 (Dec. 16, 2009), http://www.sec.gov/rules/final/2009/33-9089.pdf.

208. Aguilar, *supra* note 204.

209. *Id.*

210. *Id.*; *see also* ADAM SEDGEWICK, NAT'L INST. OF STANDARDS & TECH., CYBERSECURITY FRAMEWORK, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

211. Seth Berman & Valérie Imparato, *Data Breaches and the Board Room*, CORP. BOARD MEMBER, https://boardmember.com/data-breaches-boardroom/ (last visited Apr. 7, 2020).

212. *See, e.g.*, Aguilar, *supra* note 204 (citing a 2013 survey finding that companies that detected more incidents and reported lower average financial losses per incident employed a full-time chief information security officer (or equivalent) who reported directly to senior management).

cost-effective to outsource cybersecurity to a third-party firm that specializes in such work.[213]

Finally, boards must develop clear and coherent disclosure policies. These plans should include how cyber-attacks will be disclosed internally to employees and externally to customers, investors, and any regulatory agencies. Boards should consider the SEC's disclosure guidance. As Commissioner Aguilar advised, companies should disclose breaches that put customer data at risk, even in the absence of materially adverse impact to the company.[214] This serves the function of allowing victims of the breach an opportunity to protect themselves by promptly authorizing their customer data to be frozen to minimize potential damage, among other purposes. Another consideration is transparency may result in goodwill among consumers and the industry.

2. Have a Plan, Stick to it, and Make Sure it Works

Companies must become doomsday preppers. Cyber-attacks occur in unpredictable fashions with varying degrees of impact on the target company. The most important procedure that companies can have is a disaster plan. Companies must not only plan for the worst but also make sure to test, update, and ensure company compliance.

Businesses must first identify their "crown jewels," or the information, assets, and services demanding the most protection.[215] Companies should consider how these items are collected and protected, while recording the physical, administrative, and technical safeguards in place for handling sensitive information.[216] For example, does the company assign passwords and usernames for handling certain information? If so, then to whom? Are these passwords and usernames frequently changed? If any, what encryption standards does the company employ?[217] What is the extent of employee training related to data security and company polices? Is data accessible to third-parties? How are these relationships terminated, and when is confidential information destroyed? In answering these questions, companies hone in on the internal and external cyber-risks that the security plan will ultimately address. The board should then delegate responsibility to employees, who can then make informed determinations as to what an action plan will consist of and its implementation.

---

213. Shipley, *supra* note 72.

214. Aguilar, *supra* note 204.

215. U.S. DEP'T OF JUSTICE, CYBERSECURITY UNIT, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS 2 (Apr. 2015), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

216. Patricia Bailin & Arielle Brown, *Preparing for a Data Breach: Data Security Regulations and Best Practices*, 32 WESTLAW J. COMPUTER & INTERNET, at *4 (2015).

217. *See also* Anna Murray, *How Not to Be Victim of a Cyber-Attack: Security Rules for Lawyers*, 255 N.Y.L.J., June 1, 2016, at 4, 8. (recommending companies to "[t]ake a look at [their] forms, logins, and password-recovery practices" to avoid falling victim to hacker attacks).

Once a plan is developed, it is imperative for companies to conduct frequent testing of these procedures. To this end, companies can conduct cyber-drills, which are simulated attacks that test organizational response.[218] These drills prepare employees in the event of an attack, identify chinks in existing plans, and allow for evaluation of the existing system's stringency. Cyber-drills test the most important areas of breach response: efficiency and timing of harm mitigation, call centers' ability to handle an influx of customer inquiries, and the capability of employees to keep detailed records of the breach in preparation for any post-attack litigation or regulatory concerns.[219] Testing allows companies to update their plans based on any perceived weaknesses before the stakes become catastrophic.

In addition to implementation and testing, the company should ensure compliance as a going concern. One way companies can achieve this goal is through employee training. Regular training educates staff as to company-wide prevention, detection, and cyber-threat response.[220] IT professionals should also conduct periodic evaluations that look at the changing threat landscape, areas of weakness, and the degree of compliance with the existing system. Also, insurance and cybersecurity firms can conduct audits of the company.[221] These findings must be communicated up the chain-of-command, through senior management, and ultimately, to the board on a regular basis.

3. Key Practical Recommendations for Any Cybersecurity Plan

Within this general framework, there are several practical precautions that companies can implement to fortify cybersecurity defense systems.

Businesses must maintain strong passwords that include numerous characters and are frequently changed. All computer screens should have these passwords. Users should be prompted to input passwords whenever computers have not been used for a reasonable amount of time. Finally, passwords should not be maintained in files on company computers or on other documents that are readily accessible. Companies should also develop policies for erasing usernames and passwords of terminated employees.

Encryption programs can secure data known to have a high risk of unauthorized exposure.[222] Encryption "involves running a readable message

218. Bailin & Brown, *supra* note 216, at *5.

219. *Id.*

220. The SEC's Division of Investment Management issued guidance in April 2015, suggesting frequent employee training as to cyber threats, prevention, detection, and response at registered investment companies. All companies should follow this advice. *See* U.S. SEC. & EXCH. COMM'N, DIV. OF INV. MGMT., IM GUIDANCE UPDATE NO. 2015-02: CYBERSECURITY GUIDANCE 2 (Apr. 2015), http://www.sec.gov/investment/im-guidance-2015-02.pdf.

221. Susskind, *supra* note 61, at 613.

222. MEGAN COSTELLO, 1 DATA SEC. & PRIVACY LAW § 3:31 (2015).

known as 'plaintext' through a computer program that translates the message according to an equation or algorithm into unreadable 'ciphertext.'"[223] This process effectively encodes data to ensure that only authorized users are able to "decrypt" encrypted messages into plaintext using a compatible "key."[224] Both physical property, such as thumb drives and laptops, and wireless networks should be protected with encryption codes. Information that is backed up in a cloud should also be encrypted.

Companies must avoid sharing encryption access codes with employees and third-party vendors, thus limiting access only to essential personnel. When encryption codes are provided to staff, logs should be maintained to track this information and ensure that when employees are terminated so too is their access.

Companies should also establish programs that continuously monitor network activity to detect red flags and access points for cybercriminals.[225] These logging programs gather information about normal network activity and alert IT professionals when users engage in irregular access throughout the company.[226] This allows companies to stamp out potential attacks before they spread.

The company must stay abreast of the constantly changing threat landscape. This will entail meeting with law enforcement officials, monitoring network activity, and holding regular discussions with staff to strategize for crisis management and post-disaster continuity.

All companies should obtain cyber-insurance. As of 2018, over five hundred carriers offer these policies.[227] Cyber-insurance allows companies to obtain financial coverage for the various expenses commonly resulting from data breaches, including costs related to reputational harm, business interruptions, and breach response and notification obligations.[228] In addition to cyber-insurance, some companies might consider directors and officer's liability insurance to shoulder costs related to defending derivative suits and regulatory actions.[229]

223. Bernstein v. U.S. Dep't of State, 974 F. Supp. 1288, 1292 (N.D. Cal. 1997).

224. *Id.*

225. U.S. DEP'T OF JUSTICE, *supra* note 215, at 3.

226. Shields, *supra* note 11, at 368.

227. *State of the Cyber Insurance Market—Top Trends, Insurers and Challenges: A.M. Best*, INS. J. (June 18, 2019), https://www.insurancejournal.com/news/national/2019/06/18/529747.htm.

228. *See Top 3 Reasons Firms Are Buying Cyber Insurance*, INS. J. (June 12, 2015), http://www.insurancejournal.com/news/national/2015/06/12/371607.htm.

229. William T. Um & Paul T. Moura, *Shareholders and Regulators Clamp Down on Boards Over Corporate Governance of Cyber Risk*, 21 WESTLAW J. DERIVATIVES 1, 4 (Jan. 16, 2015).

4. Contracting with Third-Party Vendors

Another way to mitigate cyber-risk is due diligence and accurate draftsmanship of agreements with third-party vendors.[230] Companies should make several considerations when scouting potential vendors. These factors include the vendor's limitations on data access by employees, virus protection, and data encryption strategies, as well as business recovery practices and program coding methodologies.[231] Once businesses determine that a vendor's cyber-controls meet company standards, they may address any remaining concerns by contract.

There are several provisions companies should consider when drafting contractual agreements governing the nature of the vendor relationship:[232]

- Clearly define the term "breach" as it relates to the data and systems involved in the relationship.
- Consider non-disclosure or confidentiality agreements to ensure that information obtained under the contract will not be shared with any extraneous parties.
- Develop clear contractual language related to data storage, retention, and delivery. This must describe how company data is stored and transmitted while in the vendor's systems, including any encryption requirements.
- Include right-to-audit clauses that give the company the ability to perform physical audits of the vendor's data storage and controls.
- Identify the type and location of servers used and the extent of recovery safeguards.
- Address the manner and timing when the vendor notifies the company of a breach and the party responsible for notifying customers.
- Include limits on vendor-employee access and obligations upon termination of the relationship.

Cyber-attacks are inevitable and unpredictable. However, companies that combine due diligence, comprehensive agreements, and the practical recommendations discussed above will be better prepared in the event of a breach.

230. FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES 26 (Feb. 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

231. *Id.* at 26.

232. The suggested contractual terms provided in this paragraph are drawn largely from the 2015 FINRA Report's discussion on vendor management and contracting. *Id.* at 26–30.

B. INCIDENT AND THREAT RESPONSE

In many instances, only a cross-departmental cyber-crisis response will uncover the true extent of an attack's organizational impact. Response teams must eliminate the security breach as quickly as possible and recover any purloined data. Later, companies should enlist employees from various departments to correct the long-term, enterprise-wide concerns over the ensuing weeks and months.

1. Immediate Action Steps

Once an attack is underway or discovered, the business must activate its company-wide incident response program. The company must conduct a preliminary investigation to determine the validity, source, and scope of a purported attack. Sound network logging capabilities are crucial in making these determinations, and businesses must ensure that such monitoring programs are in place prior to an attack.[233] The DOJ recommends using log information to isolate the affected systems, the origin of the intrusion, any malware used or remote servers to which data were sent, and if possible, the identity of any other victim organizations.[234]

How a company bottles up the breach may take many forms depending upon the type of attack and its size. For example, companies may need to filter out a DDoS attack, or in the case of an intrusion, block further illegal access or monitor the activity to further understand the scope of the infiltration.[235] Other responses include rerouting network traffic, abandoning the network, and restoring it to a prior state (provided there is a backup).[236]

In addition to stopping the breach and preventing further infiltration, response teams should document the steps taken in remedying the situation. Recording the procedures followed after a breach informs future responses and aids potential litigation or regulatory investigations. Similarly, companies should not delete suspicious files or data cybercriminals stored on the network to orchestrate their attack.[237] Companies should maintain any relevant files and communications, and avoid modifying data.[238] The DOJ recommends maintaining forensic images of the affected computers in order to preserve a record of the system at the time of the incident.[239] A sound incident response plan will delegate the responsibility of retaining custody of these records prior to the attack.

233. U.S. DEP'T OF JUSTICE, *supra* note 215, at 6.
234. *Id.* at 7.
235. *Id.*
236. *Id.* at 7–8.
237. *Id.* at 7.
238. *Id.*
239. *Id.* at 8.

2. Assessing Legal Implications

Once the breach is stopped, the company must begin assessing the broader organizational concerns beginning with any legal and regulatory implications. As soon as possible, the legal team should take the lead in meeting with management, IT, and compliance professionals to determine the extent of the breach. This will be necessary for informing any disclosure obligations and potential regulatory exposure. The company must also consider and anticipate any private liability causes of actions that are likely to flow from the cyber-attack, including the common theories of liability discussed *supra* Section I.C.2., and begin mounting a defense to any such complaints. Spoliation may be the third rail for fending off these claims, so evidence collected in response to the breach needs to be preserved at all costs.

While the company will likely be the target of post-breach litigation or regulatory scrutiny, it is critical not to forget that these businesses are victims. Companies may pursue claims against their attackers under federal statutes, such as the SCA or EEA. Organizations may also wish to pursue common law claims under state property or trade secret law. If the cybercriminal is an employee, then the company can consider an action relying on that (former) staff member's terms of employment.[240]

In most cases, however, it will be in the company's best interest to forego affirmative litigation following a cyber-attack. From a practical perspective, the ability to bring any such litigation hinges on identifying the perpetrators. Cybercriminals are often difficult to track as they may be anonymous actors, sophisticated criminal organizations, or even nation states.[241] Moreover, litigation may not be in a company's best interest from a public relations or financial perspective. Publicizing the breach may diminish customer goodwill, divert resources and employee time, as well as harm shareholder value.[242] Instead, companies may be better off consulting with law enforcement officials, such as the FBI, immediately after the cyber-incident. Law enforcement may work with the company to conduct a discreet investigation without further disruption of business operations.[243] These government enforcement agencies may rely on authorities and investigative tools not accessible to private organizations.[244]

3. Notification

Following a cybersecurity breach, a company's first set of notifications should always be made to its personnel. The extent of information relayed

240. Breaux et al., *supra* note 79, at 26.

241. *See, e.g.*, Jorge Contreras et al., *Mapping Today's Cybersecurity Landscape*, 62 AM. U. L. REV. 1113, 1114 (2013).

242. Breaux et al., *supra* note 79, at 26.

243. U.S. DEP'T OF JUSTICE, *supra* note 215, at 10.

244. *Id.* at 11.

may vary depending on whether employee information was compromised, and whether the company plans to disclose the incident to the public or regulators. A second–but critical–party that companies must inform is law enforcement. Developing a rapport with law enforcement may assist in apprehending the attackers. Moreover, once alerted, these officials may heighten surveillance to potentially prevent further attacks.[245]

A company might be under existing obligations to notify under federal law (such as the GLBA) or a state notification law. Disclosure might be required pursuant to SEC guidelines. In such cases, timely notification is a foregone conclusion. Even if a company is not formally obligated to do so, it should consider reaching out to the SEC, FDIC, or relevant governing agency. This allows the business to share concerns over the nature of the breach and any unresolved disclosure issues.

Regarding post-breach notification procedures, companies must keep in mind that the cover up is always worse than the crime—or negligent conduct. Businesses should be upfront and timely in disclosing a significant breach to the public. Prompt notification to harmed parties—customers or employees—may mitigate the threat of lawsuits or at least lessen damages. When notifying the public, companies must ensure that customer support is in place to respond to inquiries about the incident. Companies should have answers as to how it will respond in the future to further breaches, and the steps it has taken to prevent the most common types of breaches. Maintaining a coherent and unified tone to the public is also critical in holding onto shareholders after a significant breach.[246]

4. "Failure Isn't Fatal, but Failure to Change Might Be":[247] Learning from the Post-Breach Investigative Process

The post-breach investigative process is crucial to fulfilling several important goals. The business must fully understand the attack to make tangible improvements to the company's policies and response plans. Developing a clear timeline of the events precipitating the attack allows companies to focus on and correct technical vulnerabilities in IT systems. Confirming the source of the breach might result in an alteration of

245. Companies should create positive relationships with enforcement agencies and engage in "cyber outreach and information sharing programs sponsored" by government agencies. *See* Edward J. McAndrew, *Perspective: How Companies Can Work with the U.S. Government on Cybersecurity Threats*, BLOOMBERG L. (Apr. 1, 2016), https://biglawbusiness.com/perspective-how-companies-can-work-with-the-u-s-government-on-cyber-threats/.

246. *See* Melissa Sawyer & Audra Cohen, *Five Issues Directors of Consumer and Retail Companies Should Consider Immediately Following a Cybersecurity Breach*, BLOOMBERG BNA (July 20, 2015), https://www.sullcrom.com/files/upload/Bloomberg_Cybersecurity_Sawyer_Cohen_2015.pdf.

247. This quote comes from coaching legend John R. Wooden. *See The Wizard's Wisdom: 'Woodenisms'*, ESPN (June 4, 2010), https://www.espn.com/mens-college-basketball/news/story?id=5249709.

employment policies or network monitoring procedures. It may also underscore the importance of developing an ongoing, collaborative relationship with law enforcement.

The board must work with management and across departments to discuss the execution of its post-breach response. It should focus on if the organization followed its disaster plan and identifying any gaps between the actual response and the procedures outlined in the plan. A dialogue with staff must ascertain why procedures were missed, if they were missed, and how to prevent these omissions in the future. Companies should consider hiring an objective third-party to conduct these investigations, including but not limited to law firms, cybersecurity firms, or consultants that specialize in the area.

III. IMPROVING CYBERSECURITY: CURRENT DEBATE & POSSIBLE SOLUTIONS

Due to recent data intrusions at government agencies and private companies, cybersecurity has catapulted to the top of Congress' list of legislative priorities. The House of Representatives and Senate have considered three significant bills related to cybersecurity. The Protecting Cyber Networks Act (PCNA) and National Cybersecurity Protection Advancement Act of 2015 (NCPAA) were recently passed in the House. The Cybersecurity Information Sharing Act (CISA) passed in the Senate in October 2015.[248] Although these bills have key differences, they share similar approaches; that is, information sharing between the government and private entities must be encouraged, facilitated, and legally protected if we want to win the war against cybercrime. The following discussion summarizes the core components of each piece of legislation while an evaluation of their benefits and costs will follow.

A. WILL CONGRESS TAKE THE OFFENSIVE? THE CURRENT DEBATE OVER INFORMATION SHARING LEGISLATION

1. The House Bills: The Protecting Cyber Networks Act & The National Cybersecurity Protection Advancement Act of 2015

Together, the two House bills authorize and provide liability protections for the sharing of cyber-threat data between private companies and the government. The first bill, the PCNA passed by a 307-116 margin on April

248. Eric Geller, *Senate Passes Major Cybersecurity Info-Sharing Bill CISA*, DAILY DOT (Oct. 27, 2015), https://www.dailydot.com/debug/cisa-senate-passage-cybersecurity-information-sharing-act-congress/.

22, 2015.[249] The PCNA authorizes voluntary sharing of cyber-threat indicators or defensive measures between private companies and various government agencies.[250] Before sharing data, a company must "take reasonable efforts" to remove what it reasonably believes to be personally identifiable information unrelated to a cyber-threat.[251] Federal entities must make similar efforts. Moreover, the PCNA requires the Privacy and Civil Liberties Oversight Board to report to Congress and the President every two years as to the sufficiency of procedures to address privacy and civil liberties concerns.[252] Companies that, in good faith, share information in accordance with the procedures outlined in the bill avoid civil liability.[253]

The NCPAA passed the following day by a 355-63 vote.[254] The NCPAA is generally similar to the PCNA but for the fact that it authorizes sharing exclusively between private entities and the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCIC).[255] Another crucial difference lies in the type of criminal behavior the government can prosecute under each bill. The NCPAA authorizes the Secretary of DHS to use information obtained through its procedures to investigate and prosecute a limited category of offenses: (1) criminal computer fraud, (2) imminent threat of death or serious bodily harm, (3) a serious threat to a minor, or (4) an attempt or conspiracy to commit any of such offenses.[256] In contrast, the PCNA allows agencies receiving information, pursuant to its provisions, to prosecute a broader range of offenses, including fraud and identity theft, espionage and censorship, or trade secret theft.[257]

Under the NCPAA, private companies can also conduct network awareness of their IT systems without civil liability.[258] Network awareness is defined as scanning, identifying, acquiring, monitoring, logging, or analyzing information that is stored on, processed by, or transiting an information system.[259] Like the PCNA, the NCPAA contains a number of privacy

249. Natasha G. Kohne et al., *Senate Passes Burr-Feinstein Cybersecurity Bill*, AKIN GUMP (Oct. 28, 2015), https://www.akingump.com/en/experience/practices/corporate/ag-deal-diary/senate-passes-burr-feinstein-cybersecurity-bill.html.

250. *See* H.R. 1560, 114th Cong. § 102 (2015) (promoting "timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal government agencies, or state, tribal, or local governments").

251. H.R. 1560, § 203.

252. *Id.* at § 107(b)(1)(A).

253. *Id.* at § 106.

254. Cat Zakrzewski, *House Passes Complementary Cyber Information-Sharing Bill*, TECHCRUNCH (Apr. 23, 2015), https://techcrunch.com/2015/04/23/house-passes-complementary-cyber-information-sharing-bill/.

255. H.R. 1731, 114th Cong. § 2 (2015).

256. H.R. 1560, 114th Cong. § 233(b)(3).

257. *See* H.R. 1731, 114th Cong.

258. *Id.* at § 3.

259. *Id.* at § 2(a)(8).

protections, which, if followed in good faith, may preclude civil liability. [260] Companies must, prior to sharing, take reasonable efforts to safeguard and remove personally identifiable information unrelated to cyber-risks.[261] The NCIC must do the same prior to sharing.

2. The Senate Bill: The Cybersecurity Information Sharing Act

Like the two House bills, the Senate's CISA[262] seeks to encourage sharing of cyber-threat data between private companies and the government. As with the PCNA and NCPAA, information sharing under CISA is voluntary. Private entities may also monitor and operate defensive measures to detect, prevent, or mitigate cyber-threats on their own IT systems, as well as the systems of other entities if provided written consent.[263] Moreover, the Senate bill allows government agencies to use shared information not only to prosecute cybercrimes, trade secret theft, and economic espionage but also terrorist attacks that may lead to imminent death, serious bodily or economic harm, or procurement of a weapon of mass destruction.[264]

CISA requires companies and the government to prevent unauthorized access to and "scrub" personally identifiable data from the shared information.[265] It also provides liability protection for companies that comply with the bill's procedures.[266] Companies that exchange threat indicators or assistance relating to prevention, investigation, or mitigation of cyber-threats are exempt from private antitrust suits so long as sharing is for cybersecurity purposes.[267] This exemption is inapplicable to otherwise collusive behavior, such as price-fixing or exchanging price or cost information, customer lists, or data about future competitive planning.[268]

3. Arguments For and Against Proposed Cybersecurity Legislation

At the heart of the debate over these proposed cybersecurity bills lies the age-old tradeoff between autonomy and privacy on the one hand and security on the other. Opponents of CISA, PCNA, and NCPAA believe the bills threaten privacy and civil liberties while undermining, rather than enhancing, cybersecurity. Supporters argue that facilitating timely information sharing

260. *Id.*
261. *Id.*
262. S. 754, 114th Cong. (2015).
263. *Id.* at § 104.
264. *Id.*
265. *Id.*
266. *Id.* at § 106.
267. *Id.* at § 104.
268. S. 754, 114th Cong. (2015).

of cyber-threats is the best way to enhance U.S. cybersecurity without unduly trampling on citizens' civil liberties.

A chief fear is that the bills would expand unauthorized monitoring of users' online activities.[269] Others worry that the proposed legislation is overbroad as it authorizes information sharing to prevent crimes not limited to cybersecurity, such as terrorism or imminent bodily harm.[270] Despite these concerns, there is also doubt that increased data sharing will address the root cause of cybersecurity attacks; for example, in a survey of IT professionals, 87% stated that more information sharing would not significantly reduce privacy breaches.[271] To some, amalgamating data from various sources could have the unintended consequence of creating an attractive, one-stop target for cybercriminals.[272] Currently, there are at least twenty federal information-sharing offices.[273] Between 2006 and 2013, however, the number of federal information security failures has increased by over 1,000%.[274] The government's inability to secure the data it collects under existing sharing mechanisms casts further doubt on the bills' effectiveness.[275]

Proponents of the bills acknowledge that information sharing is by no means a panacea. While stopping every possible intrusion is probably an untenable goal, pooling of cyber-threat data greatly improves the government and private sector's ability to thwart catastrophic data breaches. Information sharing enables IT experts to analyze a larger data set, thus enhancing the detection and advanced warning of cyber-attacks.[276] Many companies avoid sharing information about cyber-threats with one another and the government

269. *See* Andy Greenberg, *CISA Cybersecurity Bill Advances Despite Privacy Concerns*, WIRED (Mar. 3, 2015, 7:18 PM), http://www.wired.com/2015/03/cisa-cybersecurity-bill-advances-despite-privacy-critiques/; *Coalition Letter From 55 Civil Society Groups, Security Experts, and Academics Opposing PCNA*, ACLU (Apr. 21, 2015), https://www.aclu.org/sites/default/files/field_document/pcna_letter_final.pdf.

270. *Coalition Letter From 55 Civil Society Groups, Security Experts, and Academics Opposing PCNA*, *supra* note 269.

271. Andrea Castillo, *Cybersecurity Bill More Likely to Promote Information Overload than Prevent Cyberattacks*, THE HILL (May 7, 2015, 1:00 PM), http://thehill.com/blogs/congress-blog/homeland-security/241242-cybersecurity-bill-more-likely-to-promote-information.

272. *Id.*

273. *Id.*

274. Eli Dourado & Andrea Castillo, *Federal Cybersecurity Breaches Mount Despite Increased Spending*, MERCATUS CTR., GEO. MASON U. (Jan. 20, 2015), http://mercatus.org/publication/federal-cybersecurity-breaches-mount-despite-increased-spending; *Federal Agencies' Cybersecurity Failures Leaving Americans' Personal Information at Risk*, SECURITY Mag. (Jun. 26, 2019), https://www.securitymagazine.com/articles/90436-federal-agencies-cybersecurity-failures-leaving-americans-personal-information-at-risk.

275. Castillo, *supra* note 271; s*ee generally* COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK (2019), https://www.portman.senate.gov/sites/default/files/2019-06/2019.06.25-PSI%20Report%20Final%20UPDATE.pdf.

276. Andrew Tannenbaum, *To Prevent Cyberattacks, Share the Threat Data*, WALL ST. J. (July 9, 2015), http://www.wsj.com/articles/to-prevent-cyberattacks-share-the-threat-data-1436482349.

for fear of liability.[277] Thus, proponents of the bills argue liability protections are necessary to incentivize meaningful information sharing.

Those who support these bills assert that the privacy and civil liberties arguments are overblown, if not red herrings. According to Andrew Tannenbaum, cybersecurity counsel at IBM, personally identifiable data plays no role in the detection of cyber-threats.[278] Rather, technical data must be shared to fend off cyber-attacks, and the bills contain robust protections which ensure that it is exclusively this type of data that is shared. Before sharing information, companies must "scrub" or remove personally identifiable information unrelated to cyber-risks. The government, upon receipt, then initiates a second scrubbing. Failure to comply with these privacy protections may preclude reliance on liability safe harbors.[279]

B. RECOMMENDATIONS

1. Information Sharing Legislation with Built-In Privacy Protections

Congress must enact comprehensive cybersecurity legislation that facilitates information sharing between private entities and the government. Provisions similar to those outlined in the PCNA, NCPAA, and CISA should be adopted as they strike the right balance between encouraging data sharing that strengthens our cybersecurity infrastructure while providing reasonable protections that safeguard individual privacy.

This legislation should expressly authorize voluntary sharing of technical, non-personally identifiable information between companies and with the government. When threat indicators are shared, companies and the government would be better positioned to detect and ultimately defend against potential cyber-attacks.

The cyber-threat landscape is complex and constantly changing. It demands that companies and the government be able to rapidly communicate best practices, threats, and vulnerabilities in a timely manner and without fear of liability. This is no secret. The White House,[280] a bipartisan coalition in

277. S. Rep. No. 114–32, at 3 (2015) (Conf. Rep.); *see also* Jennifer Steinhauer, *House Passes Cybersecurity Bill After Companies Fall Victim to Data Breaches*, N.Y. TIMES (Apr. 22, 2015), http://www.nytimes.com/2015/04/23/us/politics/computer-attacks-spur-congress-to-act-on-cybersecurity-bill-years-in-making.html?_r=0.

278. Tannenbaum, *supra* note 276.

279. *See* H.R. 1560, 114th Cong. § 106 (2015); H.R. 1731, 114th Cong. § 3 (2015).

280. Jeh Johnson, *Federal Cybersecurity Needs Improvement*, POLITICO (July 13, 2015), http://www.politico.com/magazine/story/2015/07/federal-cybersecurity-needs-improvement-120061.html#.VbATsipVikq; Press Release, Grant Schneider, Fed. Chief Info. Sec. Officer and Senior Dir. for Cybersecurity Policy, President Trump Unveils America's First Cybersecurity Strategy in 15 Years (Sep. 20, 2018), https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/; *see also, e.g.*, COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, supra note 275, at 3 (2019).

Congress,[281] the U.S. Chamber of Commerce Leadership Council,[282] and major software developers,[283] such as Apple, IBM, and Microsoft, each support data sharing legislation as a necessary tool to combat today's cyber-threat climate.

This legislation must contain safeguards that ensure personal information is not shared without authorization. Initially, the type of information shared should be limited to technical data. To guarantee this outcome, entities must first determine if information is reasonably related to cybersecurity threats or defenses. If the data is relevant, all personally identifiable elements must be removed before sharing. Information will then undergo a second scrubbing by the recipient. Any liability protections will be pre-conditioned on a good faith attempt to comply with these procedures. Finally, an objective third-party, such as the Privacy and Civil Liberties Oversight Board, can report bi-annually on any privacy concerns.[284]

Information sharing is not the be-all-end-all solution to today's cyber woes. To fortify cybersecurity systems, this legislative solution should be considered alongside implementing many of the recommended cyber-strategies already discussed. Top-down, cross-departmental cybersecurity procedures, disaster plans, encryption, strong password protection, employee education, and network monitoring are some of the many tools that should be used to buttress the proposed legislation.

2. A Federal Data Breach Notification Standard

Congress must enact a clear, coherent federal data breach notification standard. There is currently no uniform data breach notification standard. Rather, all fifty states maintain their own notification statutes.[285] The current mélange of state data breach notification laws poses a serious problem for both companies and consumers. When a business suffers a breach, it must first determine if it is under a legal duty to notify customers. This decision is made unduly complicated, costly, and often ambiguous because fifty states

281. *See* Press Release, Comm. on Homeland Sec., Bipartisan Cybersecurity Bill Overwhelmingly Passes House (Apr. 23, 2015), https://homeland.house.gov/news/legislation/bipartisan-cybersecurity-bill-overwhelmingly-passes-house.

282. The Leadership Council is made up of Chamber of Commerce businesses, including Alliance of Automobile Manufactures, Blackberry, CTIA-The Wireless Association, Duke Energy, National Cable and Telecommunications Association, Retail Industry Leaders Association, The Boeing Company, J.P. Morgan Chase, and many others. *See* Aaron Boyd, *New Cybersecurity Council Backs Info Sharing Legislation*, FED. TIMES (July 7, 2015, 2:39 PM), http://www.federaltimes.com/story/government/cybersecurity/2015/07/07/cybersecurity-leadership-council/29814101/.

283. *See* Victoria Espinel, *Effective Information Sharing Legislation Needed to Combat Cyber-Attacks*, HUFFINGTON POST (July 22, 2016, 10:59 AM), http://www.huffingtonpost.com/victoria-espinel/effective-information-sha_b_7848378.html.

284. *See generally History and Mission*, PRIVACY & C.L. OVERSIGHT BOARD, https://www.pclob.gov/about/ (last visited Mar. 17, 2020).

285. *See, e.g.*, NAT'L CONF. ST. LEGISLATURES, supra note 122.

currently have their own notification laws.[286] Not only must a company decide which laws apply, it must make difficult interpretations under the various state notification statutes since they are constantly changing.[287] Moreover, most state notification statutes conflict on key issues, such as length of time required to notify parties and the definition of what constitutes a breach.[288] This lack of uniformity demands a clarified solution.

Fortunately, a White House proposal provides the framework for shaping a federal notification standard.[289] The proposal applies to businesses that use, access, transmit, store, dispose of, or collect sensitive, personally identifiable information of over 10,000 individuals during any twelve-month period.[290] In the event of a breach, these entities must provide notice to affected individuals without "unreasonable delay," or within thirty days.[291] A breach is generally defined as any compromise of data resulting in unauthorized acquisition of personal information.[292] Importantly, companies are not required to notify individuals if there is no risk of harm or fraud to customers.[293] Businesses would also have to provide notice to DHS whenever a breach affects more than 5,000 individuals.[294]

The White House proposal contains a series of exemptions. Notice is not required if the FBI or Secret Service determines that notification of the breach "could be expected to cause damage to the national security."[295] Notification is also excused, if upon conducting a risk assessment that is submitted to the FTC, the business determines that there is "no reasonable risk that a security breach has resulted in, or will result in, harm to affected individuals."[296] Finally, entities are exempt from notification if they utilize security programs that effectively block the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are

286. *Id.*

287. Divonne Smoyer & Christine Nielsen Czuprynski, *47 Attorneys General to Congress: Federal Breach Legislation Should Not Preempt the States*, REED SMITH: GLOBAL REGULATORY ENFORCEMENT BLOG (July 8, 2015), http://www.globalregulatoryenforcementlawblog.com/2015/07/articles/data-security/47-attorneys-general-to-congress-federal-breach-legislation-should-not-preempt-the-states/.

288. *See* Mary Bono, *The Need for a National Data Breach Notification Law*, THE HILL (Jan. 20, 2015, 6:00 AM), http://thehill.com/blogs/pundits-blog/technology/229968-the-need-for-a-national-data-breach-notification-law.

289. *See* H.R. 3806, 115th Cong. (2015).

290. *See* H.R. 1704, 114th Cong. § 101(a) (2014) (as proposed by President Obama). Incorporated into H.R. 1865, 116th Cong. *See H.R. 1865: Further Consolidated Appropriations Act, 2020*, GOVTRACK, https://www.govtrack.us/congress/bills/116/hr1865.

291. *See* H.R. 1704.

292. *Id.* at § 1(g)(1).

293. *Id.* at § 101(a).

294. *Id.* at § 106(a).

295. *Id.* at § 102(a).

296. This assessment must include detailed logging data covering at least six months prior to submission. H.R. 1704, 114th Cong. § 102(b) (2014).

charged to the account of the individual.[297] Under this third exemption, companies must still provide notice to affected customers if a security breach results in any fraud or unauthorized transactions.[298]

A serious point of friction lies in the federal proposal's interaction with state notification laws. Under the proposal, federal law would preempt any state law relevant to "notification by a business entity engaged in interstate commerce of a security breach of computerized data."[299] State attorneys general have overwhelmingly opposed this facet of the federal proposal.[300] Many do not want to lose the flexibility to craft more or less stringent notification standards commensurate with their state's needs.[301]

This proposed legislation was introduced under former President Obama and has been reintroduced under President Trump.[302] The legislation was initially introduced following the Equifax data breach in 2017.[303]

While its exact terms will be debated, there is no question that the time is ripe for a uniform data breach notification standard. A federal standard will provide certainty to a murky area of the law and make compliance with notification requirements less costly and complex for businesses. This will prevent undue fines against companies which fail to comply with complex and frequently changing state notification laws.

The varied, conflicting, and fluctuating nature of state notification statutes harms almost every business, not only large corporations. Almost all companies now offer and sell their goods or services over the Internet to consumers around the world. Moreover, smaller companies are most prone to suffer a cyber-attack.[304] It adds an unnecessary expense upon these companies, which have just suffered a breach, to determine if they must notify customers under each potentially relevant state notification law. A uniform federal notification standard will streamline this process and cut undue expenses. These costs are better off allocated for spending on IT personnel and defense systems. Without question, consumers will also benefit from a clear federal standard. When companies can be certain that

297. *Id.* at § 102(c)(1)(A).

298. *Id.* at § 102(c)(1)(B).

299. *Id.* at § 109.

300. Cory Bennett, *State AGs Clash with Congress Over Data Breach Laws*, THE HILL (July 7, 2015, 5:32 PM), http://thehill.com/policy/cybersecurity/247118-state-ags-warn-congress-against-preempting-data-breach-laws.

301. *See id.*

302. *See* Personal Data Notification and Protection Act of 2017, H.R. 3806, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/house-bill/3806/text.

303. Press Release, Jim Langevin, U.S. Congressman, Langevin Reintroduces the Personal Data Notification and Protection Act (Sept 18, 2017), https://langevin.house.gov/press-release/langevin-reintroduces-personal-data-notification-and-protection-act.

304. *See* Scott Steinberg, *Cyberattacks Now Cost Companies $200,000 on Average, Putting Many Out of Business*, CNBC (Oct. 13, 2019), https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html.

notification is required, those citizens, whose information has been compromised, will be promptly informed.

3. Clearer SEC Guidance on "Materiality" of Cyber Risks and Incidents

The SEC is currently considering additional guidance to the newly issued guidance on cybersecurity disclosures.[305] Under SEC rules, registered companies must file annual and quarterly reports as well as updates following any material changes or harm to the company.[306] While the SEC does not provide direction as to what constitutes a "cyberattack," it requires companies to disclose cyber-risks and incidents that are or will likely be material.[307] Materiality as it relates to cybersecurity is a misleading term. Material harm is often evaluated in terms of financial impact.[308] In addition to non-financial material breaches, companies are not required to disclose mere infiltrations or failed attempts.[309] While such events might not be sufficiently material to warrant SEC disclosure, they are surely matters of concern to most investors.

There is a clear disincentive for companies to report failed breach attempts or threats. Such disclosure could be unduly costly to companies and create exposure to greater liability. The risk and costs associated with even an attempted cyber-attack are great even if no customer or employee information is compromised. Although no one advises non-reporting, an attempted attack may damage share price or be used to drum up a potential shareholder lawsuit.[310] Clearly, the result of cybersecurity attack may result in the quintessential "a rock and a hard place" decision.

Some still resist the notion that the SEC should be tasked to implement new disclosure requirements whenever a matter becomes of great public

305. *See SEC Confirms Plans to Issue New Cybersecurity Disclosure Rules*, ALSTON & BIRD: PRIVACY & CYBERSECURITY BLOG (Apr. 27, 2015), http://www.alstonprivacy.com/sec-confirms-plans-to-issue-new-cybersecurity-disclosure-rules/; *Spotlight on Cybersecurity, the SEC and You*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/spotlight/cybersecurity (last visited Apr. 9, 2020).

306. Cory Bennett, *SEC Weighs Cybersecurity Disclosure Rules*, THE HILL (Jan. 14, 2015, 6:00 AM), http://thehill.com/policy/cybersecurity/229431-sec-weighs-cybersecurity-disclosure-rules.

307. WGL HANDBOOK SEC ACCT. & DISCLOS. pt. E24.2, at *1 (Thomson Reuters ed. 2015); Ken Tysiac, *How Should Materiality Be Applied? FASB Weighs In*, J. ACCT. (Sept. 24, 2015), https://www.journalofaccountancy.com/news/2015/sep/fasb-proposal-what-materiality-means-201513079.html; *To Disclose or Not to Disclose—Applying the Concept of Materiality to Financial Statement Disclosures*, WIPFLI LLP (Jan. 4, 2016), https://www.wipfli.com/insights/articles/aa-disclose-or-not-disclose-applying-concept-of-materiality.

308. David B.H. Martin et al., *SEC Activity Trends in Cybersecurity and Securities Law*, INSIDE COUNSEL (Apr. 14, 2015), http://www.insidecounsel.com/2015/04/14/sec-activity-trends-in-cybersecurity-and-securities; Tysiac, *supra* note 307; *To Disclose or Not to Disclose—Applying the Concept of Materiality to Financial Statement Disclosures*, *supra* note 307; *Spotlight on Cybersecurity, the SEC and You*, supra note 305.

309. Martin et al., supra note 308.

310. Bennett, *supra* note 307.

concern. Increased reporting of non-material cybersecurity-related information might only add to the length and prolixity of disclosure documents without benefitting investors.[311]

At the same time, there are many valid criticisms of current cybersecurity disclosure rules. Some contend that companies will only disclose breaches related to theft of customer or employee information, but the same companies will not report other critical breaches. For example, those breaches resulting in theft of trade secrets, other intellectual property, or corporate plans.[312] Moreover, when companies do make cybersecurity disclosures, they often do so in a non-specific, boilerplate manner that is useless to investors, employees, and consumers.[313] From a practical perspective, it might be difficult for companies to determine whether a cybersecurity issue is material. As Congressmen Jim Langevin and Jim Hines point out, the materiality of a cyber-related issue is hard to assess because "the effects [of a cyber-breach] are often not distinguishable from the many confounding variables surrounding a company's earnings."[314] Given the elusiveness of this definition and the risks associated with reporting cybersecurity threats, companies will likely err on the side of non-disclosure.

The quality of a company's cybersecurity and data protection is of cardinal importance to investors. Additionally, consumers and the general public benefit from such information. Cybersecurity has become one of the most significant dangers facing today's businesses. It is arguably on par with the many financial and operational risks companies face. To make informed decisions, investors should be made aware of a business' cyber-vulnerabilities and the steps being taken towards mitigating these risks.

The non-investing consumer also benefits from increased cybersecurity disclosures. When companies must report on their cyber-controls, vulnerabilities, and defenses, they are more prone to take cybersecurity seriously. This incentivizes improved cyber-measures that better secure costumer information. The growing risk of cyber-theft in today's business climate coupled with the many benefits associated with reporting of cyber-related issues makes regulatory action a no-brainer. The Commission should take this opportunity to make the necessary updates to its cybersecurity disclosure rules.

311. *See* Roberta Karmel, Comm'r, U.S. Sec. & Exch. Comm'n, Cybersecurity Roundtable at the Washington, D.C. SEC Headquarters 114 (Mar. 26, 2014) (transcript available on SEC website).

312. *See* Douglas Meal, Partner, Ropes & Gray LLP, Cybersecurity Roundtable at the Washington, D.C. SEC Headquarters 106 (Mar. 26, 2014) (transcript available on SEC website).

313. Bennett, *supra* note 307.

314. Nelson, *supra* note 66.

CONCLUSION

"[T]here are only two types of companies: those that have been hacked and those that will be."[315] By now this quote from former FBI Director Robert Mueller has become gospel. JEEP, JP Morgan, Adobe, SONY, the U.S. Government's Office of Personnel Management, and the Houston Astros are victims of cybercrime. Truly, no business or organization is safe from a cyber-attack. As the issues discussed in this Article demonstrate, we are a long way from where we need to be in order to adequately address these growing threats. Nevertheless, there are several steps within reach that will significantly bolster our cybersecurity infrastructure. Today's cyber-threat landscape demands multi-faceted solutions. Implementing the steps recommended in this Article ensure that the United States is moving in the right direction to prevent the growing and catastrophic threat posed by today's cybercriminals.

315. Mueller, supra note 1.