UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 19 | Issue 1 Article 18

3-1-2015

Cybersecurity: Recognizing the Risk and Protecting Against Attacks

Kristin Shields

Cybersecurity: Recognizing the Risk and Protecting Against Attacks

I. INTRODUCTION

In April 2014, JPMorgan Chase ("JPMorgan") CEO Jamie Dimon warned that even though in 2014 alone the company would spend $250 million and assign 1,000 people to addressing cybersecurity issues, the protections still may not be enough to protect the company from cyberattack.[1] Dimon's fears came to fruition just months later when JPMorgan and at least twelve other financial institutions[2] became victims of a series of coordinated hacking attacks.[3]

In the cyberattack on JPMorgan, hackers accessed the bank's network through a JPMorgan employee's personal computer.[4] From there, hackers infiltrated the bank's computer systems and gained access to over ninety of the bank's servers.[5] From June to August of 2014, the attack went undetected, and hackers accessed JPMorgan's network through a security flaw on one of the bank's websites.[6] Similar to other

1. Doug Carroll, *Banks Admit Growing Cyberattack Risks*, USA TODAY (Aug. 28, 2014, 4:06 PM), http://www.usatoday.com/story/money/business/2014/08/28/banks-growing-cyber-security-risks/14741653/.

2. Andy Peters, *Morning Scan: Cyberattacks Spread; Geithner and 'Loan Sharky'*, AM. BANKER (Oct. 10, 2014, 9:00 AM), http://www.americanbanker.com/bankthink/morning-scan-cyberattacks-spread-geithner-and-loan-sharky-1070431-1.html ("Others in the hackers' crosshairs may have included mutual fund giant Fidelity Investments, online brokerage E*Trade Financial, payroll giant Automatic Data Processing and banks Citigroup, Regions Financial and HSBC.").

3. Nicole Perlroth, *JPMorgan and Other Banks Struck by Hackers*, N.Y. TIMES (Aug. 27, 2014), http://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html?_r=0.

4. Emily Glazer & Danny Yadron, *J.P. Morgan Says About 76 Million Households Affected by Cyber Breach*, WALL ST. J. (Oct. 2, 2014, 9:32 PM), http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372.

5. Jessica Silver-Greenberg et al., *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES DEALBOOK (Oct. 2, 2014, 12:50 PM), http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/.

6. Jordan Robertson & Michael Riley, *JPMorgan Hack Said to Span Months via Multiple Flaws*, BLOOMBERG (Aug. 29, 2014, 8:54 AM), http://www.bloomberg.com/news/2014-08-29/jpmorgan-hack-said-to-span-months-via-multiple-flaws.html.

recent attacks, the attack on JPMorgan involved a message that tricked customers into clicking on a false link that appeared to be a secure link from JPMorgan.[7] For over a decade, cybercriminals have been using this technique, known as "phishing," to steal customers' identification and account information through a fake website or email.[8] The JPMorgan attack, however, included new technical elements as well.[9] When customers clicked the link, the hackers not only accessed JPMorgan's systems through the fake login page, they also installed malware on the users' computers that could help them hack into other institutions.[10]

By infiltrating over ninety of JPMorgan's servers, hackers obtained "high-level administrative privileges in the systems" and accessed customer accounts.[11] The attack on JPMorgan compromised or even lost a large number of sensitive data files.[12] While no evidence existed of fraudulent activity pertaining to the data breach, the compromised data consisted of customers' contact information, including names, addresses, phone numbers, and email addresses.[13] The attack affected an estimated 76 million households and 7 million businesses.[14] In the months following the attack, regulators and prosecutors, including the Federal Bureau of Investigation ("FBI"), the National Security Agency ("NSA"), the Department of Homeland Security ("DHS"), the U.S. Attorney's Office in Manhattan, and New York's Department of Financial Services ("DFS"), began to investigate

7. Joseph Steinberg, *Why You Are at Risk of Phishing Attacks (and Why JP Morgan Chase Customers Were Targeted Last Week)*, FORBES (Aug. 25, 2014, 8:31 AM), http://www.forbes.com/sites/josephsteinberg/2014/08/25/why-you-are-at-risk-of-phishing-attacks-and-why-jp-morgan-chase-customers-were-targeted-this-week/.

8. *See* Avivah Litan & John Pescatore, *What to Do Right Now About Phishing*, AM. BANKER, May 21, 2004, at 11 (defining "phishing" as "using fake e-mails and Web sites to steal account and ID information" and suggesting that phishing was a threat to online banking in 2004).

9. Steinberg, *supra* note 7.

10. *Id.*

11. Nicole Perlroth & Matthew Goldstein, *After Breach, JPMorgan Still Seeks to Determine Extent of Attack*, N.Y. TIMES (Sept. 12, 2014), http://www.nytimes.com/2014/09/13/technology/after-breach-jpmorgan-still-seeks-to-determine-extent-of-attack.html?_r=0.

12. Michael Riley & Jordan Robertson, *FBI Said to Examine Whether Russia Tied to JPMorgan Hacking*, BLOOMBERG (Aug. 27, 2014, 5:04 PM), http://www.bloomberg.com/news/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking.html.

13. JPMorgan Chase & Co., Current Report (Form 8-K) (Oct. 2, 2014).

14. *Id.*

and analyze the breadth of the attack and the motive behind it.[15]

While historically regulators only responded to security incidents after they occurred, recently regulators at both the federal and state level intensified their scrutiny of financial services companies' cybersecurity preparedness.[16] The Securities Exchange Commission ("SEC") conducted cybersecurity examinations of more than fifty broker-dealers in 2014.[17] The Federal Financial Institutions Examination Council ("FFIEC") conducted cybersecurity assessments of 500 community banks.[18] The State of New York conducted targeted cybersecurity preparedness assessments of the banks it regulates.[19] Additionally, the Financial Industry Regulatory Authority ("FINRA") sent letters to roughly twenty broker-dealers seeking information on how they manage cybersecurity threats.[20]

Federal and state agencies also suggested ways for financial institutions to protect against cyberattacks.[21] For example, in June 2013, the Office of the Comptroller of the Currency ("OCC") hosted a webinar to educate community banks on cybersecurity standards.[22] In addition, in 2014 the National Institute of Standards and Technology ("NIST") created the Framework for Improving Critical Infrastructure Cybersecurity ("Framework").[23] The Framework aims to help guide industries as they improve their cybersecurity efforts[24] by identifying

15. Emily Glazer et al., *Hackers May Have Targeted at Least 13 Firms*, WALL ST. J. (Oct. 8, 2014, 9:32 PM), http://online.wsj.com/articles/citigroup-regions-financial-e-trade-adp-saw-traffic-linked-to-j-p-morgan-hackers-1412783395.

16. Sanford Reback, *Financial Industry in the Cyber Crosshairs: BGOV Analysis*, 15 Computer Tech L. Rep. (BNA), No. 16, at 411, 411 (Aug. 15, 2014).

17. *Id.*

18. *Id.*

19. *Id.*

20. *Id.*

21. Press Release, U.S. Dep't of the Treasury, In Call to Action, Treasury Secretary Lew Urges U.S. Financial Sector To Redouble Efforts Against Cyber Threats (July 16, 2014), http://www.treasury.gov/press-center/press-releases/Pages/jl2571.aspx.

22. Press Release, Office of the Comptroller of the Currency, OCC Holds Web Conference for Community Banks on Cyber Threats (June 12, 2013), http://www.occ.gov/news-issuances/news-releases/2013/nr-occ-2013-96.html.

23. The NIST Framework is the guidance created in response to Executive Order 13636. NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. The Framework is meant to assist organizations in managing cybersecurity risk. *Id.*

24. Joe Adler, *Banking Groups Hail New Federal Cybersecurity Steps*, AM. BANKER, Feb. 13, 2014, at 20.

best practices for cybersecurity protection and creating a common mechanism to evaluate and discuss those practices.[25]

Despite regulatory pressure and financial institutions' efforts to protect against security threats, sophisticated cyberattacks against financial institutions occur every day, and the resulting costs have become part of the business.[26] While data breaches and cyberattacks were once just a possibility to financial institutions and other businesses, the question has evolved from a matter of "whether" to "when."[27] Even with regulators paying more attention to the cyberthreats facing financial institutions,[28] the threat to an institution's reputation and the possibility of losing customers' trust should motivate financial institutions to proactively improve their cybersecurity infrastructure.[29]

As the risk of cyberattacks increases, banks, both large and small, should use the newly available guidance to identify weaknesses in their infrastructure and develop a proactive security posture.[30] This Note proceeds in six parts. Part II details the mechanics behind cyberattacks.[31] Part III identifies the effects of cyberattacks on financial institutions.[32] Part IV discusses the legal liability of financial institutions following a cyberattack.[33] Part V evaluates regulatory efforts to increase cybersecurity requirements and prevent cyberattacks.[34] Part VI suggests solutions financial institutions may use to protect against cyberattacks.[35] Finally, Part VII concludes by

25. NAT'L INST. OF STANDARDS & TECH., *supra* note 23, at 1.

26. Mike Snider & Kevin Johnson, *New Cyberattack on Banks 'Very Sophisticated'*, USA TODAY (Aug. 28, 2014), 7:55 PM), http://www.usatoday.com/story/money/business/2014/08/28/jpmorgan-chase-bank hack/14730183/.

27. Elizabeth E. McGinn et al., *The Board of Directors and Cybersecurity: Setting up the Right Structure*, 103 Banking Rep. (BNA) No. 8, at 458, 458 (Aug. 26, 2014).

28. Rachel Witkowski, *Policymakers Preaching About Cybersecurity, But Are Banks Listening?*, AM. BANKER, July 1, 2013, at 7.

29. Jackie Stewart, *Cybersecurity Threats Demand Small-Bank Directors' Attention*, AM. BANKER, Aug. 27, 2014, at 4.

30. Earl Crane, *Cybersecurity Framework Can Help Banks Address Increased Regulatory Scrutiny*, AM. BANKER (Feb. 26, 2014, 10:00 AM), http://www.americanbanker.com/bankthink/cybersecurity-framework-can-help-banks-address-regulatory-scrutiny-1065839-1.html.

31. *See infra* Part II.

32. *See infra* Part III.

33. *See infra* Part IV.

34. *See infra* Part V.

35. *See infra* Part VI.

emphasizing the importance of financial institutions using the available guidance to make sure that their networks are sufficiently protected.[36]

II. HOW CYBERATTACKS OCCUR

Cybercriminals can access computer systems and business networks in a variety of ways.[37] The most common methods include phishing, malware, and accessing the unsecure networks of third-party vendors.[38]

A. Phishing

Phishing is when a cybercriminal sends an email, text, or pop-up message asking for personal or financial information.[39] A phishing message may say something like, "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."[40] The goal of a phishing message is to deceive the recipient into believing that the message comes from a legitimate business and entering personal information based on their belief.[41] Once the recipient provides the information, the hacker can then use the information to commit fraud.[42] The attack on JPMorgan included a phishing campaign targeting JPMorgan customers.[43] JPMorgan customers received emails that appeared to be from JPMorgan instructing the recipient to click a link.[44] Once a recipient clicked on the link, the security of the user's computer was compromised.[45]

36. *See infra* Part VII.

37. KASPERSKY LAB, GLOBAL IT SECURITY RISKS 2014 – ONLINE FINANCIAL FRAUD PREVENTION 1, 10 (2014), *available at* http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Financial_Security_report.pdf?_ga=1.34870177.1093389152.1412952265.

38. *Id.*

39. *Phishing*, FED. TRADE COMM'N (Sept. 2011), http://www.consumer.ftc.gov/articles/0003-phishing.

40. *Id.*

41. *Id.*

42. *Id.*

43. *Smash & Grab Campaign Targets JP Morgan Chase Customers*, PROOFPOINT, http://www.proofpoint.com/threatinsight/posts/smash-and-grab-jpmorgan.php (last visited Jan. 8, 2015).

44. *Id.*

45. *Id.*

B. Malware

After phishing compromises a user's computer, cybercriminals can install malware.[46] Cybercriminals can install malware, short for "malicious software," on computers, smart phones, or other mobile devices without the owner's consent.[47] Once malware is installed, cybercriminals can monitor and control online activity, steal confidential information, and commit fraud.[48] In the JPMorgan attack, after a customer clicked the phishing link, the hackers installed malware on the user's computer.[49] By installing the malware, hackers accessed JPMorgan's computer network, including servers that contained customers' personal information.[50]

C. Third-Party Vendors

Financial institutions often use third-party vendors such as law firms, accounting firms, marketing firms, maintenance companies, and janitorial companies for necessary services.[51] Some of these third parties' security practices are remiss or even nonexistent.[52] As a result, even if cybercriminals cannot directly breach a financial institution's network, they may still gain access to the institution's network through the network of a third-party vendor.[53] For example, in the 2013 attack on Target ("Target Breach"), cybercriminals accessed Target's computer system through the security system of a heating and cooling contractor who was working for Target.[54] Once the cybercriminals accessed Target's network through the third-party vendor, they were able to install malware on the company's computer servers and steal

46. *Malware*, FED. TRADE COMM'N (Feb. 2014), http://www.consumer.ftc.gov/articles/0011-malware.

47. *Id.*

48. *Id.*

49. *Smash & Grab Campaign Targets JP Morgan Chase Customers*, *supra* note 43.

50. Glazer & Yadron, *supra* note 4.

51. Jessica Silver-Greenberg & Matthew Goldstein, *After JPMorgan Chase Breach, Push to Close Wall St. Security Gaps*, N.Y. TIMES DEALBOOK (Oct. 21, 2014, 4:57 PM), http://dealbook.nytimes.com/2014/10/21/after-jpmorgan-cyberattack-a-push-to-fortify-wall-street-banks/?_php=true&_type=blogs&_r=0.

52. *See id.* ("In attack after attack, hackers are rebuffed by financial institutions, only to slip through the cracks at vendors, including some that have virtually no security.").

53. *Id.*

54. *Id.*

confidential credit and debit card data as well as Target customers' personal information.[55]

III. EFFECT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS

When a data breach occurs, the cost falls onto American consumers and their financial institutions.[56] Depending on the size of the breached company, the cost of a single data breach can range anywhere from $66,000 to $938,000 per organization.[57] The cost of a breach includes actual fraud losses, the price of reissuing cards, loss of customers, the burden on customer service, and fees paid to consultants and lawyers who banks hire to manage the problem.[58] Another cost for the breached institution, though difficult to quantify, involves the strain put on employees' productivity following a data breach. [59]

The National Association of Federal Credit Unions estimated that the 2013 Target Breach[60] cost the financial institutions of affected customers a combined $480 million in fraud loss, reimbursement costs, card replacement costs, operational costs, and other associated expenses.[61] After the Target Breach, an American Bankers Association survey found that the loss per fraudulently used debit card averaged $331 while the loss per credit card was $530.[62] Customers are not liable for paying these fraudulent charges and reissue costs.[63] Instead, the

55. Elizabeth A. Harris et al., *A Sneaky Path into Target Customers' Wallets*, N.Y. TIMES, Jan. 18, 2014, at A1.

56. Carrie Hunt, *Retailers Should Be Held to Stricter Standards on Data Security*, AM. BANKER (Aug. 27, 2014, 10:00 AM), http://www.americanbanker.com/bankthink/retailers-should-be-held-to-stricter-standards-on-data-security-1069613-1.html.

57. The cost depends on the size of the institution. Penny Crosman, *How Much Do Data Breaches Cost? Two Studies Attempt a Tally*, AM. BANKER, Sept. 12, 2014, at 4. The smaller amount corresponds to smaller institutions and the bigger amount corresponds to larger institutions. *Id.* However, larger institutions tend to have economies of scale that make the cost per customer lower for larger institutions than for smaller institutions. *Id.*

58. *Id.*

59. *Id.*

60. The Target Breach began "with a malware-laced email phishing attack sent to employees at an HVAC firm" that Target used as a third-party vendor. *Target Hackers Broke in Via HVAC Company*, KREBS ON SEC. (Feb. 5, 2014, 1:52 PM), http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

61. Hunt, *supra* note 56.

62. AM. BANKERS ASS'N, TARGET BREACH IMPACT SURVEY 10 (July 2014), *available at* http://www.aba.com/Tools/Function/Payments/Documents/TargetBreachBankImpact.pdf.

63. Press Release, Target, Target Provides Update on Data Breach and Financial Performance (Jan. 10, 2014), http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance.

burden falls on banks to pay the costs and then seek reimbursement from merchants.[64]

Reissuing debit and credit cards following a data breach also creates expenses for banks.[65] For large banks,[66] reissuing a new debit card costs about $2.70 while reissuing a new credit card costs about $2.99.[67] For small banks,[68] however, reissuing a new debit card costs about $11 while reissuing a new credit card costs about $12.75.[69] Small banks incur higher costs because they must reissue all potentially affected cards as a precaution, whereas large banks have resources such as contact centers that can actively monitor potentially affected cards and reissue only those that are fraudulently used.[70] In addition, large banks' economies of scale help lower the per-unit cost of replacing each fraudulently used card.[71]

Even when banks receive reimbursement from a merchant following a breach, the amount reimbursed usually does not cover the total cost of the breach, including card reissuance and fraud loss.[72] In breaches that occurred between 2009 and 2014, less than 34% of all banks received any amount of reimbursement; 100% of large banks received at least some reimbursement following a data breach, compared to only 25% of small banks.[73] Even still, the majority of banks that received any sort of reimbursement received less than ten cents per dollar, and even worse, almost 50% of banks received less than one cent per dollar.[74]

Breaches also impact consumers.[75] When a breach occurs,

64. Lawrence Delevingne, *Banks May Take Their Pound of Flesh from Target over Breach*, NBC NEWS (Dec. 23, 2013, 3:19 PM), http://www.nbcnews.com/business/business-news/banks-may-take-their-pound-flesh-target-over-breach-f2D11794859.

65. AM. BANKERS ASS'N, *supra* note 62, at 5–16.

66. For purposes of the study, large banks were defined as banks with more than $50 billion in assets. *Id.* at 6.

67. *Id.* at 11.

68. Small banks were defined as banks with less than $1 billion in assets. *Id.* at 6.

69. *Id.* at 11. ("Included are costs for mailing, card stock, and additional staff resources, etc. Because many respondents were unable to track additional staff time spent to respond to customer inquiries and to monitor and prevent fraud related to the Target breach, the reissue costs reported here are conservative, baseline figures.").

70. Crosman, *supra* note 57.

71. *Id.*

72. AM. BANKERS ASS'N, *supra* note 62, at 20.

73. *Id.* at 18–19.

74. *Id.* at 21.

75. *Id.* at 13–14.

customers, especially those who possess only one card, are inconvenienced when they must wait for a replacement card before they can make purchases.[76] Additionally, following a breach, customers face an increased risk of fraud and future identity theft.[77] Thus, a company's failure to protect against a data breach results in lost business, which could ultimately negatively affect the company's valuation.[78]

A financial institution's data breach may result in a loss of both individual and business customers.[79] Although customers do not always cite a data breach as their reason for leaving a bank,[80] research conducted by SafeNet, Inc. found that 80% of individual customers were at least somewhat unlikely to do business with a company that experienced a data breach of financial information.[81] Further, a study conducted by the Kaspersky Lab found that 60% of personal customers opted for an online store or financial services provider that offers safeguards for protecting financial information, and 75% of customers would prefer to have all of their devices protected by their banks against online financial fraud.[82] Similarly, a separate study conducted by the Kaspersky Lab concluded that almost half of businesses changed banks after security breaches compromised their accounts.[83] Of the businesses surveyed, 82% admitted that they would consider leaving a bank that suffered a breach.[84] Thus, data breaches cause customers to lose trust in breached companies.[85]

Following a breach, the biggest cost to financial institutions is arguably the burden on customer service.[86] Within twenty-four hours of

76. *Id.*

77. Letter from Tim Pawlenty, President and CEO, Fin. Servs. Roundtable, to Members of Congress (Jan. 27, 2014), *available at* http://fsroundtable.org/open-letter-congress-cybersecurity-01-27-14/.

78. *Global Survey Reveals Impact of Data Breaches on Customer Loyalty*, SAFENET, http://www2.safenet-inc.com/email/2014/dp/GlobalCustomerSentiment/index.html#1918 (last visited Jan. 29, 2015).

79. Crosman, *supra* note 57.

80. *Id.*

81. Global Survey, *supra* note 78.

82. KASPERSKY LAB, CONSUMER SECURITY RISKS SURVEY 2014: MULTI-DEVICE THREATS IN A MULTI-DEVICE WORLD 22 (July 2014), *available at* http://media.kaspersky.com/en/Kaspersky_Lab_Consumer_Security_Risks_Survey_2014_ENG.pdf.

83. Crosman, *supra* note 57.

84. *Global IT Security Risks 2014*, *supra* note 37, at 14.

85. Global Survey, *supra* note 78.

86. Crosman, *supra* note 57.

learning of a breach, some banks begin calling customers to notify them.[87] While some banks use third-party vendors to handle these calls at call centers, at some small and mid-size banks, the burden falls on bank employees.[88] Each of these customer service calls can cost up to $20.[89] Even for banks that use third-party vendors, each call can cost as much as replacing the card.[90] In addition to calls, banks also draft and send letters to customers regarding the breach.[91] If customers become aware of the breach by the media or other outside sources, they will call the bank inquiring about unauthorized transactions or requesting a new card.[92] When breaches occur, bank employees and call centers can become overwhelmed, which may hinder the bank's normal operations and its customer service center's ability to provide assistance.[93] After the Target Breach, for example, at least one bank reported that employees were removed from performing their usual duties to assist with customer service and notification procedures.[94] Following a breach, employees may get fired, and, in the most severe instances, the morale of an organization may never recover.[95]

IV. POTENTIAL LEGAL LIABILITY OF FINANCIAL INSTITUTIONS FOLLOWING A CYBERATTACK

When a data breach occurs, companies can expect lawsuits for negligence, breach of contract, and violation of state laws including deceptive trade practices acts or data breach notification laws.[96] These suits can also result in personal liability for the directors of the bank.[97]

When a cybersecurity breach harms customers, affected customers may likely bring negligence claims against the institution.[98]

87. AM. BANKERS ASS'N, *supra* note 62, at 14.

88. *Id.* at 13–14.

89. Crosman, *supra* note 57.

90. As a reminder, the cost to reissue a card can range from $2.70 to $12.75 per customer. AM. BANKERS ASS'N, *supra* note 62, at 14.

91. *Id.* at 13.

92. *Id.* at 14.

93. Crosman, *supra* note 57.

94. AM. BANKERS ASS'N, *supra* note 62, at 13.

95. Crosman, *supra* note 57.

96. Kimberly Peretti, *Cyber Threat Intelligence: To Share or Not to Share—What Are the Real Concerns*, Banking Daily (BNA), Issue No. 173 (Sept. 8, 2014).

97. McGinn et al., *supra* note 27, at 461.

98. Joe Adler, *Why Obama's 'Voluntary' Cybersecurity Plan May Prove Mandatory*,

After a Home Depot data breach in 2014 compromised the personal information of 56 million customers, the company faced at least fifteen lawsuits alleging that Home Depot acted negligently by failing to adequately secure the customers' personal and financial information.[99] When faced with negligence claims, institutions must show that their cybersecurity procedures are "commercially reasonable."[100] The reasonableness standard is subjective, and although the Framework is not a requirement for institutions, courts are likely to use it to determine reasonable industry practices.[101] Thus, if an institution's cybersecurity practices do not align with the Framework, the institution must prove that its practices are nevertheless reasonable.[102]

Financial institutions may also face breach of contract suits in which customers allege that the institution contractually promised to protect the customer's personal information and then breached that promise.[103] In a class action lawsuit against eBay in 2014, plaintiffs alleged breach of contract based on the terms of the company's privacy policy, as well as breach of implied contract based on customers' disclosure of information in reliance on the company's stated privacy policy to protect against data breaches.[104] At least one court held that a company's privacy policy or other statements made by the company assuring the security of customers' data does not constitute a contractual promise to safeguard data.[105] However, another court recognized that an implied contractual relationship may exist when a customer uses a credit or debit card at a company and expects that the company will protect its personal information.[106] Because of this undecided legal

AM. BANKER, Feb. 18, 2014, at 15.

99. Amanda Bronstad, *Lawsuits Piling Up in Home Depot Data Security Breach*, THE NAT'L L. J. (Sept. 25, 2014), http://www.nationallawjournal.com/id=1202671405651/Lawsuits-Piling-Up-in-Home-Depot-Data-Security-Breach.

100. Adler, *supra* note 98.

101. *Id.*

102. *Id.*

103. DOUGLAS H. MEAL & DAVID T. COHEN, PRIVATE DATA SECURITY BREACH LITIGATION IN THE UNITED STATES, *in* PRIVACY AND SURVEILLANCE LEGAL ISSUES: LEADING LAWYERS ON NAVIGATING CHANGES IN SECURITY PROGRAM REQUIREMENTS AND HELPING CLIENTS PREVENT BREACHES 11–12 (Aspatore 2014).

104. Complaint-Class Action ¶¶ 67–87, Collin Green, v. eBay, Inc. (E.D. La 2014) (No. 2:14-cv-01677-SM-KWR).

105. *In re* Zappos.com, Inc., No. 3:12-CV-00325-RCJ, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013).

106. Anderson v. Hannaford Bros. Co., 659 F.3d 151, 159 (1st Cir. 2011).

issue, customers may continue to allege both express and implied breach of contract claims when companies fail to reasonably protect customers' private information.[107]

When data breaches violate state laws, both the company as a whole and individual board members may be held liable[108] under deceptive trade practice acts and data breach notification statutes.[109] For example, when First National Bank of Nebraska refused to refund fees for unauthorized purchases following a data breach, the U.S. District Court for the District of Nebraska held that the bank's customers had a claim under Nebraska's Uniform Deceptive Trade Practices Act.[110] Additionally, almost all states have enacted security breach notification statutes that the state's attorney general can use to bring lawsuits against companies that fail to protect against cyberattacks.[111] Absent a federal data breach notification law, companies must comply with the requirements of state data breach notification statutes, which sometimes contradict each other.[112] Ten states, including North Carolina,[113] have statutes that explicitly allow private rights of action in addition to potential suits brought by the state attorney general.[114] Thus, after a breach, a single company may face many lawsuits for noncompliance with data breach notification statutes.[115]

Finally, when a cyberattack results in a drop in a public company's share price, shareholders may bring derivative suits against the company if it failed to adequately protect against cyberattacks.[116] When breaches compromise sensitive information, customers lose

107. Meal & Cohen, *supra* note 103, at 11–12.

108. McGinn et al., *supra* note 27, at 461.

109. Peretti, *supra* note 96.

110. Wines, Vines and Corks, LLC v. First Nat'l of Nebraska, No. 8:14-cv-00082-LES-FG3 (D. Neb. Aug. 20, 2014).

111. McGinn et al., *supra* note 27, at 461.

112. Reid J. Schar & Kathleen W. Gibbons, *Complicated Compliance: State Data Breach Notification Laws*, 12 Privacy & Sec. L. Rep. (BNA) No. 32, at 1381, 1381 (Aug. 12, 2013).

113. States explicitly allowing a private right of action include: Alaska, California, Louisiana, Maryland, New Hampshire, North Carolina, Oregon, South Carolina, Tennessee, Virginia, and Washington. *Id.* at 1384.

114. *Id.*

115. *Id.*

116. McGinn et al., *supra* note 27, at 461–62.

confidence and some may change providers.[117] As a result of this reputational damage, stock prices may drop and shareholders may sue.[118] OCC officials have warned that in order to avoid potential company and personal liability, bank boards of directors and managers must maintain adequate cybersecurity policies and practices at their institutions.[119] Boards of directors and managers should be involved in and regularly briefed about the company's cybersecurity efforts to avoid becoming an easy target for such derivative suits.[120]

V. FEDERAL AND STATE EFFORTS TO INCREASE CYBERSECURITY REQUIREMENTS AND PREVENT CYBERATTACKS

As cybersecurity has become increasingly important to the financial industry, government officials and agencies are instituting requirements and providing guidance to help improve cybersecurity policies and protect against future attacks.[121]

A. Gramm-Leach-Bliley Act

Under the Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule, financial institutions[122] have an affirmative duty to protect consumers' personal information.[123] Specifically, "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' non-public personal information."[124] Financial institutions must "establish appropriate standards . . . relating to administrative, technical, and physical safeguards to insure the security

117. *Id.* at 461.

118. *Id.* at 461–62.

119. Rachel Witkowski, *Regulators Offer Cybersecurity Guidance to Small Banks*, AM. BANKER, June 13, 2013, at 21.

120. McGinn et al., *supra* note 27, at 461–62.

121. *Cybersecurity Is Everyone's Business*, U.S. DEP'T OF HOMELAND SEC. (July 9, 2013), http://www.dhs.gov/cybersecurity-everyones-business.

122. "Financial institutions" under the GLBA include national banks, Federal branches and Federal agencies of foreign banks, member banks of the Federal Reserve System, and banks insured by the Federal Deposit Insurance Corporation. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 527(4), 113 Stat. 1338, 1449 (1999) (codified as amended at 15 U.S.C. § 6827(4) (2012)).

123. Gramm-Leach-Bliley Act § 501(a), 15 U.S.C. § 6801(a).

124. *Id.*

and confidentiality of customer records and information."[125] In addition, they are required "to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[126] To comply with GLBA's requirements, financial institutions must "develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical, and physical safeguards that are appropriate to [the institution's] size and complexity, the nature and scope of [the institution's] activities, and the sensitivity of any customer information at issue."[127] Some states have enacted legislation that extends the Safeguards Rule to state chartered banks as well.[128] A financial institution's failure to comply with the Safeguards Rule may result in charges by the Federal Trade Commission ("FTC") and significant monetary and reputational damages.[129]

B. Proposed Legislation: Cyberintelligence Sharing and Protection Act ("CISPA") and National Cybersecurity and Critical Infrastructure Protection Act of 2013

Over the last five years, almost 100 bills regarding cybersecurity have been introduced in Congress.[130] None of this proposed legislation, however, has been enacted into law.[131] While advocates of these bills stressed a need for information sharing to strengthen the security of computer networks, opponents, such as the American Civil Liberties Union ("ACLU") and other privacy advocates, feared that the bills did not adequately protect Americans' private information.[132]

125. Gramm-Leach-Bliley Act § 501(b), 15 U.S.C. § 6801(b).

126. *Id.*

127. 16 C.F.R. § 314.3 (2014).

128. *See, e.g.*, CONN. GEN. STAT. § 36a-44a (2012).

129. McGinn et al., *supra* note 27, at 460–61.

130. JAMES ARDEN BARNETT JR., RECENT TRENDS IN NATIONAL SECURITY LAW: LEADING LAWYERS ON BALANCING US NATIONAL SECURITY CONCERNS AND THE RIGHTS OF CITIZENS, *in* CYBER SECURITY: FIXING POLICY WITH NEW PRINCIPLES AND ORGANIZATION 3 (Aspatore 2014).

131. *Id.*

132. Ellen Nakashima, *Senate Intelligence Panel Advances Cybersecurity Bill*, THE WASH. POST (July 8, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/08/senate-intelligence-panel-advances-cybersecurity-bill/.

These efforts demonstrate that lawmakers recognize that issues such as cybersecurity and protection against cyberthreats require legislation, however nothing has yet been adopted.[133] Since 2013, the House of Representatives has advanced two bills regarding cybersecurity: the Cyber Intelligence Sharing and Protection Act ("CISPA"),[134] which failed, and the National Cybersecurity and Critical Infrastructure Protection Act ("NCCIP Act"),[135] which was approved by the Senate as the National Cybersecurity Protection Act in December 2014.[136] The House of Representatives passed CISPA on April 18, 2013.[137] CISPA intended "[t]o provide for the sharing of certain [cyberthreat] intelligence and [cyberthreat] information between the intelligence community and cybersecurity entities."[138] However, due to privacy concerns over proposed exceptions to existing privacy laws, the bill was not seriously considered in the Senate.[139]

Over a year later, in July 2014, the House of Representatives approved the NCCIP Act,[140] a bill that lays out security standards for federal government systems and private-sector business considered critical to the economy.[141] Most importantly, the NCCIP Act differs from CISPA in that it does not create exceptions to existing privacy laws.[142] Because of this change, some who opposed the CISPA, such as

133. Alina Selyukh, *Senate Intelligence Committee Approves Cybersecurity Bill*, REUTERS (July 8, 2014), http://www.reuters.com/article/2014/07/08/us-usa-cybersecurity-congress-idUSKBN0FD2LG20140708.

134. Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013–2014).

135. National Cybersecurity and Critical Infrastructure Protection Act of 2014, H.R. 3696, 113th Cong. (2013–2014).

136. Cory Bennett, *Senate Passes DHS Cyber Bill*, THE HILL (Dec. 10, 2014, 1:04 PM), http://thehill.com/policy/cybersecurity/226639-senate-passes-dhs-cyber-bill.

137. McGinn et al., *supra* note 27, at 462.

138. H.R. 624.

139. Victoria Finkle, *Why Cybersecurity Legislation Will Likely Come Up Short—Again*, AM. BANKER, May 28, 2013, at 12.

140. Press Release, U.S. H.R. Comm. on Homeland Security, House Passes Bipartisan Legislation to Protect Critical Infrastructure From Cyber Attack (July 28, 2014), http://homeland.house.gov/press-release/house-passes-bipartisan-legislation-protect-critical-infrastructure-cyber-attack.

141. Maria Aspan, *Bankers, When Talking Innovation, Dwell on Cyber Defenses*, AM. BANKER (Mar. 28, 2014, 7:14 PM), http://www.americanbanker.com/issues/179_60/bankers-when-talking-innovation-dwell-on-cyber-defenses-1066558-1.html.

142. Letter from Laura W. Murphy, Director of American Civil Liberties Union, to Chairmen and Ranking Members of the U.S. H.R. (Jan. 14, 2014), *available at* http://homeland.house.gov/sites/homeland.house.gov/files/images/HR3696-ACLU.pdf.

the ACLU, endorsed the NCCIP Act.[143] On July 29, 2014, the bill was referred to the Senate Committee on Homeland Security and Governmental Affairs.[144] If passed, this Act could significantly improve cybersecurity by creating the National Cybersecurity and Communications Integration Center ("NCCIC") to facilitate real-time cyberthreat information-sharing across critical infrastructure sectors.[145] It would also establish an equal partnership between private industry and the DHS to facilitate critical infrastructure protection and incident response following a cyberattack.[146]

C. NIST Guidance

As legislative attempts failed, in February 2013, President Obama issued Executive Order 13636 "to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."[147] The Executive Order directed the NIST to create a framework to reduce cyberrisks to the nation's critical infrastructure.[148] The Executive Order set out to strengthen the protections of critical infrastructure against threats of cyberattack by developing industry best practices.[149] The Order aimed to create a voluntary program to encourage financial firms, utility operators, and others who own and/or operate critical infrastructure to share information with one another about cyberthreats.[150] The voluntary program intended to promote standards that would reduce the risk of cybersecurity threats on facilities vital to national security, the economy, or public health.[151]

After a yearlong process, the NIST created the Framework as a compilation of industry best practices for managing cybersecurity risks.[152] The NIST designed the Framework to complement, rather than

143. *Id.*

144. H.R. 3696 (as passed by H.R., July 29, 2014).

145. Press Release, U.S. H.R. Comm. on Homeland Security, "National Cybersecurity and Critical Infrastructure Protection Act of 2013" (NCCIP Act) (July 29, 2014), http://homeland.house.gov/sites/homeland.house.gov/files/documents/12113_NCCIP_summary.pdf.

146. *Id.*

147. Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 12. 2013).

148. *Id.* at 11741.

149. *Id.*

150. *Id.* at 11739.

151. *Id.*

152. NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL

replace, an organization's existing cybersecurity program.[153] Ultimately, the Framework aims to assist organizations, regardless of size, degree of risk, or level of cybersecurity sophistication, in reducing and better managing their cybersecurity risks.[154]

By establishing a set of best practices, the Framework aspires to help financial institutions and other businesses set and reach their cybersecurity risk management goals in a cost-effective way, but without the increased burden of regulation.[155] While not mandatory, the Framework reflects current regulations and best practices of the financial industry and also provides guidance on how cybersecurity practices can be improved.[156] Regulators will likely use the Framework as a baseline when conducting future examinations and when updating their own examination procedures and guidance.[157]

D. OCC Guidance

The OCC's June 2013 Semiannual Risk Perspective devoted an entire section to addressing cyberthreats to banks of all sizes.[158] The report suggested that hackers might increasingly target smaller institutions that they believe lack the resources necessary to protect against cyberattacks.[159] Nevertheless, the report still identified the increasing volume and sophistication of cyberthreats as a key risk to large banks.[160] Recognizing cyberthreats as "the fastest-growing risk to banks," the OCC acknowledged that regulators currently think more in terms of supervision than in terms of regulation.[161]

The focus of the OCC policies and supervision will vary based

INFRASTRUCTURE CYBERSECURITY 11 (2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

153. *Id.* at 13.

154. *Id.*

155. Adler, *supra* note 24.

156. *Id.*

157. Crane, *supra* note 30.

158. NAT'L RISK COMM., OFFICE OF THE COMPTROLLER OF THE CURRENCY, SEMIANNUAL RISK PERSPECTIVE 7–10 (2013), *available at* http://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-fall-2013.pdf.

159. *Id.* at 7.

160. *Id.* at 9.

161. Rachel Witkowski, *OCC Sees Cybersecurity as Fastest-Growing Risk to Banks*, AM. BANKER, June 19, 2013, at 9.

on the size of the banks.[162] For example, for small to mid-size banks, the focus centers on strategic and capital planning, whereas for large banks, the focus remains "on strengthening their governance, oversight and operational risk issues."[163] Specifically, for large banks, the OCC supervisory staff will review an institution's existing threat assessment and incident response programs as well as conduct vulnerability assessments.[164] The OCC also noted that the pace of new regulatory requirements can cause increased risks for banks that do not adequately invest in cybersecurity.[165]

In addition to the Risk Perspective, the OCC hosted a webinar, attended by approximately 1,000 bankers, offering a basic course on cybersecurity policies and procedures.[166] The OCC explained that a bank's cybersecurity program should be integrated as part of its information security and vendor management processes.[167] The OCC also stressed that in order to adequately address evolving threats, a bank's cybersecurity policies and practices must be monitored and adjusted regularly.[168]

E. DFS Cybersecurity Assessments[169]

In response to the growing risk of cyberattacks against financial institutions, the New York DFS conducted an industry-wide survey on cybersecurity practices.[170] After completion of the survey in May 2014, New York Governor Andrew Cuomo announced that because of the growing risk of cyberattacks on New York banks, the DFS would begin conducting targeted cybersecurity assessments to assist banks in safeguarding personal bank records and protecting banks from

162. *Id.*

163. *Id.*

164. NAT'L RISK COMM., *supra* note 158, at 10.

165. *Id.* at 7.

166. Witkowski, *supra* note 119.

167. *Id.*

168. *Id.*

169. The DFS supervises banks, credit unions, and other financial institutions that are chartered in New York State. *Who We Supervise*, DEP'T OF FIN. SERVS., http://www.dfs.ny.gov/about/whowesupervise.htm.

170. N.Y. STATE DEP'T OF FIN. SERVS., REPORT ON CYBER SECURITY IN THE BANKING SECTOR 1 (2014) [hereinafter DFS REPORT], *available at* http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf.

cyberbreaches.[171] The new examinations will include questions regarding IT management and governance, incident response, network security, vendor management, and disaster recovery.[172] The DFS will conduct the examinations on financial institutions, including state-chartered banks, credit unions, and foreign banks whose U.S. headquarters are located in New York.[173] Each institution will be graded on its cybersecurity readiness.[174] Through the examinations, the DFS aims to support banks and help improve cybersecurity by encouraging banks to focus on their cybersecurity preparedness.[175] DFS serves as the first regulator to begin conducting regular, targeted cybersecurity preparedness assessments of the banks it regulates.[176]

F. FFIEC Guidance and Cybersecurity Assessments

In April 2014, FFIEC members[177] issued a statement notifying financial institutions of potential cyberattack risks and describing the steps institutions should take to address the attacks.[178] Then, in May 2014, the FFIEC announced plans to conduct cybersecurity risk assessments of community banks[179] to highlight areas for financial institution managers and directors to focus on to mitigate cybersecurity risks.[180] These focus areas include building a security culture,

171. Press Release, N.Y. Dep't of Fin. Servs., Governor Cuomo Announces New Cyber Security Assessments for Banks (May 6, 2014), http://www.dfs.ny.gov/about/press2014/pr1405061.htm [hereinafter DFS Press Release].

172. DFS REPORT, *supra* note 170.

173. Penny Crosman, *N.Y. Regulators Plan Heightened Scrutiny of Banks' Cyber Readiness*, AM. BANKER, May 8, 2014, at 7.

174. Id.

175. DFS Press Release, *supra* note 171.

176. Crosman, *supra* note 174.

177. The FFIEC consists of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Officer of the Comptroller of the Currency, and the Consumer Financial Protection Bureau. *Regulatory Agencies*, FED. FIN. INSTS. EXAMINATION COUNCIL, https://www.ffiec.gov/agencies.htm.

178. Advisory Letter, Fed. Fin. Insts. Examinations Counsel, Financial Regulators Release Statements on Cyber-Attacks on Automated Teller Machine and Card Authorization Systems and Distributed Denial of Service Attacks (Apr. 2, 2014), http://www.ffiec.gov/press/pr040214.htm.

179. Penny Crosman, *First Look: FFIEC Explains New Cybersecurity Assessments*, AM. BANKER, May 9, 2014, at 13.

180. Press Release, Federal Fin. Insts. Examination Council, FFIEC Promotes Cybersecurity Preparedness for Community Financial Institutions (May 7, 2014), http://www.ffiec.gov/press/pr050714.htm [hereinafter FFIEC Press Release].

identifying and monitoring risks, developing risk management processes, creating awareness and accountability, and ensuring reports to management about the institution's potential vulnerability.[181] The assessments also include examinations of the policies that community banks currently use to detect vulnerability and protect against risks.[182] The reviews focus on five key areas of cybersecurity preparedness:[183] (1) risk management and oversight; (2) threat intelligence and collaboration; (3) cybersecurity controls; (4) external dependency management; and (5) incident management and resilience.[184]

Like the Framework, the FFIEC Cybersecurity Assessment does not create new requirements for financial institutions.[185] Instead of functioning as a standalone test, the program is designed to be incorporated into the already-existing community bank examinations and to assist the relevant federal regulators in developing a baseline assessment of how banks manage cyberrisks.[186] The assessments are primarily meant to assist authorities in examining cybersecurity preparedness programs at small and mid-size banks that do not have access to all of the resources available to big banks.[187] The FFIEC's goal in conducting the assessments is to make sure that regulated financial institutions adequately manage cybersecurity risks based on their complexity and risk profile.[188] The assessment's identification of gaps in cybersecurity practices will help the FFIEC make informed decisions about future actions[189] and assist supervisors and regulators in making informed decisions to protect against cyberrisks.[190] Additionally, the assessments are designed to help FFIEC member institutions learn about the state of cybersecurity across community institutions and prioritize actions that should be taken.[191] Bank boards

181. *Id.*

182. Kristin Broughton, *FFIEC Announces Plans for Cybersecurity Assessments*, AM. BANKER, May 8, 2014, at 12.

183. Joe Adler, *How Regulators Are Shaking Up Small Bank Cyber Reviews*, AM. BANKER, June 30, 2014, at 9.

184. FED. INSTS. EXAMINATION COUNCIL, INTRODUCTION TO FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL'S CYBERSECURITY ASSESSMENT 1 (2014).

185. Adler, *supra* note 183.

186. Crosman, *supra* note 179.

187. Adler, *supra* note 183.

188. Crosman, *supra* note 179.

189. *Id.*

190. Adler, *supra* note 183.

191. FFIEC Press Release, *supra* note 180.

and management should embrace these assessments as ways to identify gaps in current practices and prepare their institution for the possibility of a cyberattack.[192]

FFIEC agencies conducted its first Cybersecurity Assessments on 500 community banks during the summer of 2014.[193] Overall, the assessments found that while the level of risk varies greatly across the financial industry, understanding the threats and techniques attackers use will help management identify, assess, and mitigate each financial institution's specific risks.[194] For example, institutions that grant employees access to the bank's network from their personal devices risk exposing their financial institution to malware.[195] The assessments also found that most financial institutions understand the need to educate employees about cybersecurity risk management, maintain event logs to understand a cyberattack after it occurs, have a process for implementing corrective controls to address previously identified vulnerabilities, and have disaster recovery plans for when incidents occur.[196] As a result of the Assessments' findings, FFIEC members must review and update current guidance to financial institutions to align it with the changing cybersecurity risk.[197]

In addition to the Assessments, a webpage launched by the FFIEC in June 2014 offers further guidance and features information about the Cybersecurity and Critical Infrastructure Working Group created in June 2013, a handbook about the FFIEC examinations, and a May 2014 webinar and video on cybersecurity for community bank CEOs.[198] These resources endeavor to assist managers and directors in understanding expectations, assessing the risks of their institution, and mitigating against those risks.[199]

192. Adler, *supra* note 183.

193. JOHN E. BOWMAN ET AL., VENABLE LLP, FINANCIAL SERVICES ALERT: FFIEC CYBERSECURITY ASSESSMENT: SENIOR MANAGEMENT MUST TAKE THE LEAD (Nov. 12, 2014), http://www.venable.com/ffiec-cybersecurity-assessment—senior-management-must-take-the-lead/.

194. FED. FIN. INST. EXAMINATION COUNCIL, CYBERSECURITY ASSESSMENT GENERAL OBSERVATIONS 4 (2014).

195. *Id.* at 1.

196. *Id.* at 4.

197. Id.

198. *Cybersecurity Awareness*, FED. FIN. INSTS. EXAM. COUNCIL, https://www.ffiec.gov/cybersecurity.htm (last visited Feb. 8, 2015).

199. Id.

VI. SUGGESTED SOLUTIONS

While financial institutions continue to develop strategies to identify and protect against cybersecurity risks, still more can be done to mitigate the risks.[200] People, whether consumers or employees, often serve as the weak link in security.[201] For example, in the JPMorgan breach, hackers used the personal computer of an employee who was working from home to access the bank's network.[202] Similarly, in the Target Breach, hackers breached Target's system using credentials stolen from an employee of the company's vendor.[203]

Educating employees and consumers on how to distinguish legitimate entities from fraudulent ones is key to protecting against phishing attacks.[204] For example, financial institutions should educate customers about the possible consequences of clicking on links or opening attachments in unsolicited emails.[205] To prevent customers from becoming a victim to these emails, financial institutions should teach their customers that banks and merchants will never ask for personal or financial information via email.[206] In addition, financial institutions should instruct customers that if they receive emails or phone calls from someone claiming to work for their bank, they should contact the bank directly to find out whether the institution actually requested the information.[207] Despite the fact that the Target Breach occurred through a third-party vendor, Target, recognizing the risk and the importance of customer education, announced plans to launch a $5 million, multiyear campaign to educate customers about cybersecurity risks, including the dangers of phishing scams.[208]

200. Penny Crosman, *A Tiny Bit of Solace for Banks in Home Depot Breach*, AM. BANKER, Sept. 10, 2014, at 1.

201. Penny Crosman, *Hacker Attack on Banks Shows Need to Lock Down Employee PCs*, AM. BANKER, Aug. 29, 2014, at 8.

202. Id.

203. Danny Yadron, Paul Ziobro & Charles Levinson, *Target Hackers Used Stolen Vendor Credentials*, WALL ST. J. (Jan. 29, 2014, 7:08 PM), http://online.wsj.com/news/articles/SB10001424052702303973704579350722480135220.

204. Steinberg, *supra* note 7.

205. Id.

206. Annamaria Andriotis, *There's a Big Data Risk for Bank Customers—And It's Not What You Think*, WALL ST. J. BLOG (Aug. 29, 2014, 8:32 AM), http://blogs.wsj.com/totalreturn/2014/08/29/theres-a-big-data-risk-for-bank-customers-and-its-not-what-you-think/.

207. Id.

208. Press Release, Target, Target Invests $5 Million in Cybersecurity Coalition (Feb.

One resource available for customer education is the FTC's Consumer Information website that provides "Examples of Phishing Messages," "How to Deal with Phishing Scams," and "Action Steps" to avoid a phishing attack.[209] The website advises consumers to neither not reply to online solicitations that ask for personal or financial information nor click on any links within those solicitations, even if they appear to be from an organization they trust.[210] As part of an effort to educate consumers, financial institutions should direct their customers to these resources, develop their own informational material, or even consider a campaign similar to Target's to disseminate the information.[211]

Financial institutions should also focus on educating and training employees.[212] Although the majority of financial institutions already train employees on cybersecurity, the benefits of such training increase when updated regularly and provided routinely.[213] Financial institutions should constantly provide employee security training, [214] and should regularly remind employees of what they should look for with respect to security threats.[215] An annual reminder to employees to be vigilant is no longer sufficient.[216] Instead, employees should be reminded about the importance of security every time they log into the system, such as through a pop-up notification requiring the user's acknowledgement before proceeding.[217] At the very least, management should brief employees about security concerns on a quarterly basis.[218] Financial institutions should present information about cyberrisks in layman's terms so that the financial institution's board of directors and team members will understand what needs to occur to properly protect against risk.[219]

18, 2014), https://corporate.target.com/discover/article/Target-to-invest-5-million-in-cybersecurity-coalit.

209. FED. TRADE COMM'N, *supra* note 39.

210. Id.

211. Steinberg, *supra* note 7.

212. Crosman, *supra* note 201.

213. FED. FIN. INST. EXAMINATION COUNCIL, *supra* note 194, at 2.

214. Andy Peters, *No One's Safe from Cyberattacks: Former Wells Fargo CIO*, AM. BANKER, Aug. 29, 2014, at 6.

215. Crosman, *supra* note 201.

216. Peters, *supra* note 214.

217. Id.

218. Stewart, *supra* note 29.

219. Id.

Financial institutions should establish programs to continuously monitor network activity to ensure that security compromises do not go undetected or unquestioned.[220] In monitoring network activity, banks should collect enough information about typical network activity so that red flags will go up if a user abnormally accesses information throughout the organization.[221] At a minimum, the institution's board of directors or board of trustees should make sure that their institutions run adequate tests on their security systems and review their security policies annually.[222] In addition, the most secure system should require employees to present a thumbprint or facial scan as evidence of their identity for authentication before accessing the network.[223] Finally, employees' access to data and programs should be limited, allowing them access only to the information that is essential for them to perform their job functions.[224]

At many institutions, directors wait until the financial institution suffers a cyberattack or attacks are otherwise widely reported to discuss cybersecurity with management.[225] However, routine discussions in board and management meetings about cybersecurity issues would strengthen risk management by building a security culture within the institution.[226] Although not mandatory, institutions should use the Framework to assess their cybersecurity risk management and help identify issues that may invite regulatory scrutiny.[227] After conducting the assessment, directors and management, particularly audit and risk committees, should be briefed on the results.[228]

Financial institutions should also develop a protocol to notify customers as soon as possible after detection of a breach.[229] In May 2014, the White House released a report encouraging banks to inform Americans when their information has been compromised or stolen.[230]

220. Crosman, *supra* note 201.
221. *Id.*
222. Stewart, *supra* note 29.
223. Crosman, *supra* note 201.
224. *Id.*
225. FED. FIN. INST. EXAMINATION COUNCIL, *supra* note 194.
226. *Id.* at 3.
227. Crane, *supra* note 30.
228. *Id.*
229. JOHN PODESTA ET AL., BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, EXECUTIVE OFFICE OF THE PRESIDENT 5 (2014).
230. *Id.* at 1.

The report recommended that Congress "pass legislation that provides for a national data breach standard" and imposes a reasonable time period for organizations to provide such notification.[231] After a cyberattack occurs, banks must disclose[232] to customers that customer data has been breached.[233] But this process can take days or even weeks.[234] Oftentimes, financial institutions and companies like Target do not immediately know what information is compromised or who is affected.[235] Cybercriminals will take advantage of these days or weeks of uncertainty by initiating a series of identity-theft scams.[236] Such scams often include emails to customers in which criminals pretend to be the financial institution whose security was compromised.[237] Nervous consumers who believe the emails often divulge the requested information and become victims of identity theft.[238]

A financial institution's delay in disclosing a breach can end up making the hacker's attempts more successful by allowing these nervous customers to become more at risk for identity theft.[239] Financial institutions should have procedures in place for notifying customers, regulators, and law enforcement when a cyberattack occurs.[240] Documentation of such procedures ensures timely notification and to assist in prompt decision-making in the event of a cyberattack.[241]

Third-party vendors also make financial institutions vulnerable to cyberattacks.[242] Institutions must examine their relationships with

231. *Id.* at 60.

232. Although companies must disclose information about a breach to customers, they are not required to disclose any information that may provide a "roadmap" for hackers to use to access a company's system in the future. Hunton & Williams, LLP, *Recent Developments Concerning Cybersecurity Disclosure for Public Companies*, PRIVACY & INFO. SEC. L. BLOG (June 24, 2014), https://www.huntonprivacyblog.com /2014/06/articles/recent-developments-concerning-cybersecurity-disclosure-public-companies/.

233. Michael Riley & Jordan Robertson, *Russian Hackers Said to Attack Five Banks Seeking Customer Data*, 19 Electronic Com. & L. Rep. (BNA) No. 34, at 1143, 1144 (Sept. 10, 2014).

234. *Id.* at 1144.

235. *Id.*

236. Andriotis, *supra* note 206.

237. *Id.*

238. *Id.*

239. *Id.*

240. FED. FIN. INST. EXAMINATION COUNCIL, *supra* note 194, at 4.

241. *Id.*

242. Stewart, *supra* note 29.

these parties to identify all potential risks.[243] For this reason, regulators now encourage banks to increase their oversight of third-party vendors.[244] As "banks increasingly rely on third-party vendors," outside vendors are gaining access to large amounts of sensitive data.[245] Some small-market firms outsource all of their information technology functions to third-party providers.[246] While financial institutions can outsource these functions, they cannot outsource the risk.[247] Outsourcing requires institutions to understand how risks are managed, and banks must have a response plan implemented in the event that data is lost or a cyberattack occurs.[248]

In addition to a bank's cyberattack response plan, institutions that use third-party vendors should ensure that any vendor they use has a plan in place to respond to a cyberthreat.[249] Therefore, before entering into a contract, management should consider the potential risks in the third-party's systems and evaluate the third-party's cybersecurity practices.[250] Financial institutions should also ensure that contracts with third parties protect the bank if a security breach occurs as a result of the relationship with the third-party.[251] Financial institutions of all sizes should use the Framework to convey cybersecurity risk management requirements to all third-parties with which they work, including providers of critical systems on which the institutions depend.[252] Using the Framework may help financial institutions avoid legal liability for negligence related to third-party relationships.[253]

With cybersecurity incidents occurring more frequently, financial institutions should obtain cyberinsurance coverage to help pay the potentially massive costs that result from a data breach.[254] While

243. *Id.*

244. *Id.*

245. Peter J. Isajiw & John C. Vázquez, *Cybersecurity Risks Reviewed—Directors and Officers Must Be Proactive and Prepared*, 13 Privacy & Sec. L. Rep. (BNA) No. 13, at 1344, 1347 (Aug. 4, 2014).

246. Adler, *supra* note 183.

247. *Id.*

248. *Id.*

249. *Id.*

250. FED. FIN. INST. EXAMINATION COUNCIL, *supra* note 194.

251. Stewart, *supra* note 29.

252. Crane, *supra* note 30.

253. Adler, *supra* note 98.

254. Kimberly Peretti & Jessica Corley, *Cybersecurity—What Directors Need to Know in an Era of Increased Scrutiny*, 13 Privacy & Sec. L. Rep. (BNA) No. 30, at 1301, 1301–07

general insurance policies may not sufficiently cover data breaches, additional stand-alone cyberinsurance plans are tailored to cover the costs of a security breach including lost income, operating expenses, and costs that arise arising out of third-party claims.[255] In addition, stand-alone cyberinsurance policies can provide coverage for both first-party losses and third-party liability.[256] Cyberinsurance policies may cover a variety of costs associated with a data breach, such as legal and investigative fees, crisis management costs, and losses due to business interruption.[257] Over 60% of risk management professionals whose company has obtained a cyberinsurance policy believe that having the insurance has improved their preparedness for handling cyberrisks.[258] However, companies purchasing cyberinsurance should consider that some policies require that legal representation come from a pre-selected panel of attorneys, so the company may not be permitted to obtain top-notch counsel should a cyberattack occur.[259]

VII. CONCLUSION

The recent attack on JPMorgan highlighted the importance of maintaining adequate cybersecurity practices for financial institutions.[260] Today, financial institutions, no matter the size, are almost certain to experience some type of cyberattack.[261] These attacks may occur through phishing, malware, or the unsecure networks of third-party vendors.[262] If successful, a single attack can cost an institution hundreds of thousands of dollars in fraud losses and other expenses.[263] It may also result in a loss of customers[264] and potential

(July 28, 2014).

255. *Id.*

256. WILLIAM T. UM, HUNTON & WILLIAMS LLP, DAILY JOURNAL: MYRIAD OPTIONS FOR CYBERINSURANCE (May 12, 2014), *available at* http://www.hunton.com/files/Publication/830fa291-8bb6-4ae6-bea6-9baa217b774c/Presentation/PublicationAttachment/1a2bcc44-24b4-4f49-8b33-14ca7a11fcbb/Myriad_options_for_cyberinsurance.pdf.

257. *Id.*

258. PONEMON INSTITUTE, MANAGING CYBER SECURITY AS A BUSINESS RISK: CYBER INSURANCE IN THE DIGITAL AGE 23 (2013).

259. *Id.*

260. Steinberg, *supra* note 7.

261. McGinn et al., *supra* note 27.

262. KASPERSKY LAB, GLOBAL IT SECURITY RISKS 2014 – ONLINE FINANCIAL FRAUD PREVENTION (2014).

263. Crosman, *supra* note 57.

264. *Id.*

lawsuits.[265] In response to the growing risk of cyberattacks, government officials and agencies have developed assessments and other guidelines to assist companies in protecting against the risk.[266] Financial institutions should use the newly available guidance to evaluate their cybersecurity practices, identify weaknesses, and ensure that their networks are adequately protected.[267]

KRISTIN SHIELDS

265. Kimberly Peretti, *Cyber Threat Intelligence: To Share or Not to Share—What Are the Real Concerns*, 103 Banking Rep. (BNA) No. 15, at 839, 839 (Oct. 21, 2014).

266. *Cybersecurity Is Everyone's Business*, DEPT. OF HOMELAND SECURITY (July 9, 2013), http://www.dhs.gov/cybersecurity-everyones-business.

267. Crane, *supra* note 30.