UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 23 | Issue 1 Article 11

3-1-2019

The Modern Threat: Data Breaches, Security Measures, and a Call for Changes

Zachary N. Layne

THE MODERN THREAT: DATA BREACHES, SECURITY MEASURES, AND A CALL FOR CHANGES

I. INTRODUCTION

Data breaches are a major threat to the public at large, and no individual or industry is safe from them.[1] In 2018, there were 1,244 data breaches, ranging in areas from banking to education and government.[2] Due to those breaches, a whopping 446 million records were stolen from individuals, including financial information and Social Security number.[3] Of the 1,244 data breaches, 135 (10.9%) fall into the banking/credit/financial category.[4] Consumers are rightfully concerned about the privacy of their data and its ability to be compromised in the event of a major breach.[5] Individuals view the compromise of their information as an infringement, and they are aware that the risk of losing personal information to malicious parties is much greater now than it ever has been due to the high frequency of data breaches in today's world.[6]

This Note focuses on recent high-profile data breaches and the questions that arise in their wake. This Note proceeds in seven parts. Part II outlines recent major data breaches that have occurred.[7] Part III uses field research to analyze and pinpoint how consumer trust is affected in a negative way when customers are confronted with a data breach.[8] Part

1. *See* IDENTITY THEFT RES. CTR., 2018 END-OF-YEAR DATA BREACH REPORT (Jan. 7, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/01/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-1.pdf (illustrating that data breaches have affected a large amount of people and virtually every industry).

2. *Id.*

3. *Id.*

4. *See id.* (defining this sector to include "entities such as banks, credit unions, credit card companies, mortgage and loan brokers, financial services, investment firms and trust companies, payday lenders and pension funds.").

5. *See FICO Survey: US Consumers Fear Bank Fraud and ID Theft More Than Terrorist Attack,* PR NEWSWIRE (July 27, 2017, 8:30 ET), https://www.prnewswire.com/news-releases/fico-survey-us-consumers-fear-bank-fraud-and-id-theft-more-than-terrorist-attack-300492706.html ("44 percent of US consumers rate identity theft and banking fraud as their top concern.").

6. *See id.* ("The loss of your personal information or money from your account cuts deep, it is a violation, and people now know it's much more likely to happen to them.").

7. *See infra* Part II (discussing recent data breaches).

8. *See infra* Part III (analyzing consumer trust after a breach).

IV identifies the common security measures used by banks and looks at new developments in cybersecurity.[9] Part V focuses on consumers' negative reactions when faced with additional security measures and the banking industry's acknowledgement that increased security measures negatively affect their customers' experiences.[10] Part VI lays out a blueprint for the future of data security, including a recommendation for federal cybersecurity regulation for the financial industry, as well as a call to require all regulators to include the Cybersecurity Assessment Tool ("CAT") as part of their examinations.[11] Lastly, Part VII concludes that these options would likely lessen the frequency of breaches.[12]

II. HISTORY OF DATA BREACHES

In December 2014, Sony Pictures "admitted to having suffered a major cybersecurity breach."[13] Hackers managed to steal and release individuals' private information and sensitive documents, which they then released to the public.[14] In the days before Thanksgiving 2014, Sony employees who attempted to access their computers were met with an unfamiliar image.[15] Over the following weeks multiple statements, allegedly from the Guardians of Peace ("GOP"), were posted online.[16] The statements were followed by links to download a large amount of information

9. *See infra* Part IV (detailing security measures commonly used).

10. *See infra* Part V (focusing on how consumers and banks feel about additional security measures).

11. *See infra* Part VI (discussing a call for change).

12. *See infra* Part VII (concluding that meaningful change could help to prevent these breaches from occurring with such great frequency).

13. Joseph Steinberg, *Massive Security Breach at Sony-Here's What You Need to Know*, FORBES (Dec. 11, 2014, 1:13 PM), https://www.forbes.com/sites/josephsteinberg/2014/12/11/massive-security-breach-at-sony-heres-what-you-need-to-know/#3d0b9c9344d8.

14. *Id.*

15. *See* Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.b658d53f0f59 ("Sony Pictures employees who tried to log into their computers were greeted with a graphic of a neon red skeleton featuring the words '#Hacked by #GOP,' and a threat to release data later that night if an unspecified request was not met.").

16. *See id.* (detailing that of the information posted online, many were "to a text-sharing site called PasteBin, which is also used by some hacktivist groups."); *see also Hacktivist*, OXFORD DICTIONARIES, https://en.oxforddictionaries.com/definition/hacktivist (last visited Jan. 29, 2019) (defining hacktivist as "A person who gains unauthorized access to computer files or networks in order to further social or political ends.").

belonging to Sony.[17] In a memo shortly after the first leak, Sony Pictures executives acknowledged the major theft of confidential data in a statement, and acknowledged that personal information could be in the hacker's hands.[18]

The banking sector was not spared, as it fell victim to a cyberattack as well.[19] In October 2014, JPMorgan "revealed that seventy-six million households and seven million small businesses may have had their private data compromised in a cyberattack."[20] In an SEC filing, JPMorgan stated that their users' personal contact information, as well as their account information, had been taken.[21] After charging the individuals responsible for the attack, the U.S. Attorney for the Southern District of New York called it "the single-largest theft of data from a U.S. financial institution."[22]

This problem has continued to rear its ugly head recently.[23] T-Mobile suffered a breach that affected two million customers, during which their personal and account information was compromised.[24] While T-Mobile was quick to alert customers that their Social Security numbers and financial information were not compromised, customers were cautioned to be on guard going forward.[25] A breach of this type has the

17. *See* Peterson, *supra* note 15 (discussing that there were "huge amounts of what appeared to be data from Sony Pictures' internal networks.").

18. *See* Peterson, *supra* note 15 ("While we are not yet sure of the full scope of information that the attackers have or might release, we unfortunately have to ask you to assume that information about you in the possession of the company might be in their possession.").

19. Sam Ro, *JPMorgan Reveals Gigantic Data Breach Possibly Affecting 76 Million Households*, BUSINESS INSIDER (Oct. 2, 2014, 4:58 PM), https://www.businessinsider.com/jpmorgan-data-breach-2014-10.

20. *Id.*

21. *JPMorgan Chase & Co.*, Current Report (Form 8-K) (October 2, 2014), https://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm; *see also id.* (detailing that the extent of the breach was "user contact information—name, address, phone number and email address—and internal JPMorgan Chase information relating to such users have been compromised.").

22. *See* Portia Crowe, *JPMorgan Fell Victim to the Largest Theft of Customer Data From a Financial Institution in US History*, BUSINESS INSIDER (Nov. 10, 2015, 10:12 AM), https://www.businessinsider.com/jpmorgan-hacked-bank-breach-2015-11 (detailing that the total number of customers affected was 83 million, according to Preet Bharara).

23. Jerry Beilinson, *Two Million T-Mobile Customers Are Hit by A Data Breach*, CONSUMER REPORTS (August 24, 2018), https://www.consumerreports.org/privacy/2-million-t-mobile-customers-hit-by-data-breach/.

24. *Id.*

25. *See id.* (stating that other threats can exist even in the absence of stolen financial information).

potential to increase vulnerability for customers.[26] While customers become most alarmed when their Social Security Number or credit card information is compromised, other stolen information can be just as detrimental to privacy.[27] For example, if a hacker obtains account information, they can send an email that looks identical to one a customer would receive from T-Mobile, containing accurate account and billing information; these are attempts to steal the customer's password, which would give the hacker full access to the online account.[28]

The aforementioned breaches only represent a small subset of the high-profile data breaches that have occurred.[29] Banks and financial institutions face an average of eighty-five breach attempts per year.[30] The average cost of a breach is around four million dollars, yet, in an industry that is as highly regulated as financial services is, the costs extend far beyond that of the average price due to consumers switching financial institutions.[31]

III. CONSUMER TRUST IN THE WAKE OF A BREACH

While overall data demonstrates that consumers are likely to discontinue the relationship with their bank after a breach, there was a slightly different result when responses were focused solely on millennials.[32] A Gallup poll revealed that an overwhelming majority of millennials are extremely trusting when it comes to companies protecting their

26. *See id.* ("In a phishing attack, criminals could send a consumer a counterfeit email—with a real account number and billing information—claiming to be from T-Mobile and asking him or her to follow a link and log in. Such an email could be an attempt to trick the consumer into revealing a password.").

27. *See id.* ("Companies are quick to reassure consumers if no Social Security numbers or credit card numbers were stolen, but other data losses can create just as much havoc," says Robert Richter, who leads privacy and security testing at Consumer Reports.).

28. *See id.* ("In a phishing attack, criminals could send a consumer a counterfeit email—with a real account number and billing information—claiming to be from T-Mobile and asking him or her to follow a link and log in. Such an email could be an attempt to trick the consumer into revealing a password.").

29. *See* IDENTITY THEFT RES. CTR., *supra* note 1 (discussing the high number of breaches that have taken place).

30. Rocco Grillo, *Regulatory Compliance Does Not Equal Cybersecurity*, CLEARING HOUSE, https://www.theclearinghouse.org/banking-perspectives/2017/2017-q2-banking-perspectives/articles/regulatory-compliance-does-not-equal-cybersecurity (last visited January 17, 2019).

31. *Id.*

32. John H. Fleming & Amy Adkins, *Data Security: Not a Big Concern for Millennials,* GALLUP (June 9, 2016), https://news.gallup.com/businessjournal/192401/data-security-not-big-concern-millennials.aspx.

information.[33] The poll results showed that millennials are much more trusting of their respective financial institutions than non-millennials (67% for millennials as compared to 56% of non-millennials).[34] The report concluded that millennials may even be naïve when it comes to the security of their online information.[35]

IV. DATA SECURITY MEASURES

The Federal Financial Institutions Examination Council ("FFIEC") was founded in 1979, pursuant to "the Financial Institutions Regulatory and Interest Rate Control Act of 1978."[36] The FFIEC is an organization tasked with creating "uniform principles, standards, and report forms for the federal examination of financial institutions."[37] An important FFIEC development relating to cybersecurity was CAT, which was unveiled in 2017.[38] The purpose of CAT is to assist organizations with identifying risks and determining the maturity of their cybersecurity measures.[39] CAT is structured as a two-step process: first, management of the organization determines its "risk profile" based on five categories: (1) Technologies and Connection Types; (2) Delivery Channels; (3) Online/Mobile Products and Technology Services; (4) Organizational Characteristics; and (5) External Threats.[40] The next step for management is to calculate their "Cybersecurity Maturity" according to five domains: (1) Cyber Risk Management and Oversight; (2) Threat Intelligence and Collaboration; (3) Cybersecurity Controls; (4) External Dependency Management; and (5) Cyber Incident Management and

33. *See id.* ("[The study] found that an impressive 80% of [millennials] say they have 'some' or 'a lot' of trust in the companies they do business with to keep their personal information secure.").

34. *See id.* ("Millennials exhibit the greatest amount of trust in their primary bank, with 67% of this group saying they have a lot of trust in this institution, compared with 56% of non-millennials.").

35. *See id.* ("[M]illennials seem to rise above [data breaches], remaining trusting—and perhaps idealistic—in the face of an abundance of evidence that their online data might not be very secure.").

36. FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, ABOUT THE FFIEC (last modified August 29, 2018, 1:11 PM), https://www.ffiec.gov/about.htm.

37. *Id.*

38. FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, CYBERSECURITY ASSESSMENT TOOL at 1 (May 2017), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf (last visited Feb. 9, 2019).

39. *Id.*

40. *Id.*

Resilience.[41] CAT is useful because it allows management to evaluate their organization's maturity levels in comparison to their risk.[42] Maturity levels rank from baseline, which constitutes the minimum expectations, to innovative, which entails creating new controls or tools.[43]

CAT was designed for institutions to assess their preparedness for breach events.[44] The FFIEC gives institutions a process capable of repetition in order to ensure they are ready in the case of an attack on their data and information.[45] While use of CAT is not required, it provides a step-by-step process that is of value to financial institutions.[46]

One common security measure used by banks and financial institutions is two-step authentication.[47] Two-step authentication is structured as follows: first, a consumer signs in with their credentials.[48] After entry of their credentials, the consumer must enter another piece of information, which usually takes the form of a code sent to a linked mobile phone.[49] The common belief of institutions is that by having this additional layer of security, hackers will be unable to access a consumer's information solely on the basis of having the consumer's password.[50] This common belief, however, may be a colossal misconception.[51]

---

41. *Id.*

42. *Id.* at 2 (detailing that it allows management to "determine whether its maturity levels are appropriate in relation to its risk. If not, the institution may take action either to reduce the level of risk or to increase the levels of maturity.").

43. *See* FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, CYBERSECURITY ASSESSMENT TOOL at 7 (May 2017), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf. (stating that the maturity levels are: Baseline, Evolving, Intermediate, Advanced, and Innovative).

44. *Id.* at 2.

45. FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, FFIEC RELEASE UPDATE TO CYBERSECURITY ASSESSMENT TOOL (May 31, 2017), https://www.ffiec.gov/press/pr053117.htm ("[The FFIEC] developed the Assessment to help financial institution management determine the institution's risk profile, inherent risks and cybersecurity preparedness. The Assessment provides a repeatable and measurable process that financial institution management may use to measure cybersecurity preparedness over time.").

46. *Id.*

47. *Two-Factor Authentication Helps Protect the One and Only You,* WELLS FARGO, https://www.wellsfargo.com/privacy-security/fraud/articles/two-factor-authentication/ (last visited February 8, 2019) (discussing how Wells Fargo uses two-factor authentication).

48. *See id.* (detailing how two-step authentication is carried out).

49. *Id.*

50. *Id.*

51. *See* Laurene Hummer, *What's Wrong with SMS Authentication? Two IBM Experts Weigh In on the NIST Recommendation*, SECURITY INTELLIGENCE (September 7, 2016), https://securityintelligence.com/whats-wrong-with-sms-authentication-two-ibm-experts-weigh-in-on-the-nist-recommendation/ (discussing the short-comings of two-step authentication when it comes to text messages).

In May 2016, the National Institute of Standards and Technology ("NIST") recommended the phasing-out of text message authentication as the second step in two-step authentication.[52] Two-step authentication falls short of absolute security due to the possibility of a consumer unknowingly downloading malware onto their phone.[53] Thus, hackers can authorize their malware to keep track of consumer text messages.[54] Even in the absence of malware, hackers can intercept and spy on text messages.[55]

A new development with a slight twist on the traditional model of two-step authentication is the advent of Duo Mobile.[56] Duo Mobile is an app for mobile devices or tablets that uses two-step authentication, but does so by the approval of push notifications rather than online insertion of a code texted to a mobile phone.[57] Users can thus thwart unauthorized attempts to access their information by simply denying the unexpected push notification that appears.[58]

The Financial Services Sector Coordinating Council has created the new "Financial Services Sector Cybersecurity Profile" as an extension of the NIST framework already in existence.[59] The profile is very flexible and adaptable, and can be used on the smallest community bank

52. *Id.*; *see also* NAT'L INST. STANDARDS AND TECH., NIST SPECIAL PUBLICATION 800-63-3, DIGITAL IDENTITY GUIDELINES (June 2017) (detailing why text message authentication is problematic).

53. *See* Hummer, *supra* note 51; *Malware*, NORTON BY SYMANTEC, https://us.norton.com/internetsecurity-malware.html (last visited Jan. 29, 2019) ("Malware is an abbreviated form of 'malicious software.' This is software that is specifically designed to gain access to or damage a computer, usually without the knowledge of the owner.").

54. *See* Hummer, *supra* note 51 ("[A] fraudster can simply command the malware to monitor text messages.").

55. Hummer, *supra* note 51.

56. *See Secure Two-Factor Authentication App*, DUO, https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile (last visited Jan. 29, 2019) ("Logging in securely is fast and easy with Duo Push, the more secure method of two-factor authentication supported by Duo Mobile.").

57. *See id.* ("Users quickly verify their identity by approving push notifications before accessing applications.").

58. *See id.* ("[Someone] can easily stop fraudulent attempts to access company data by tapping the deny button.").

59. *See* Lydia Beyoud, *Financial Industry Unveils Streamlined Cyber Compliance Standard*, BLOOMBERG LAW (October 25, 2018, 4:50 PM), https://news.bloomberglaw.com/banking-law/financial-industry-unveils-streamlined-cyber-compliance-standard-1 ("The 'financial services sector cybersecurity profile' is intended as an extension of an existing cybersecurity framework established by the National Institute of Standards and Technology (NIST).").

or the largest bank in the world.[60] In using this new profile, financial institutions can expect to reduce their compliance responsibilities between forty-nine and seventy-three percent.[61]

Wells Fargo, the third largest bank in the United States, lays out on their website precisely how they identify their customers and protect their data.[62] One of the notable features Wells Fargo employs is the use of a one-time password in order to establish identity if there is a high-risk transaction taking place.[63] An example of a high-risk transaction is sending money to an individual for the first time, or being transferred funds from a non-Wells account for the first time.[64] Moreover, in addition to the use of two-step authentication, Wells Fargo goes above and beyond with the use of biometric authentication.[65] Biometric authentication requires customers to use their fingerprints or facial features to sign into their mobile banking app.[66] When it comes to data protection, Wells Fargo has minimum encryption and browser requirements, as well as an ongoing monitoring scheme.[67] The browser requirement is designed to block older browsers that are not as secure, while the monitoring scheme will require further proof of authentication if a customer's banking transactions and behaviors sway from their usual pattern.[68]

In an interesting turn of events, banks and financial institutions are working together to assess their respective levels of preparedness for simultaneous cyberattacks.[69] In October 2018, JPMorgan Chase,

60. *See id.* ("The profile can be scaled to match a financial institution's size and needs, from community banks to the largest multinational financial institutions.").

61. *Id.*

62. Amanda Dixon, *America's Fifteen Largest Banks,* BANKRATE (February 21, 2018), https://www.bankrate.com/banking/americas-top-10-biggest-banks/#slide=1; *see How We Protect You,* WELLS FARGO, https://www.wellsfargo.com/privacy-security/fraud/protecting-you (last visited February 8, 2019) (detailing their consumer protection devices).

63. *See How We Protect You, supra* note 62 (indicating that Advanced Access is triggered when a high-risk transaction is involved); *Advanced Access Questions,* WELLS FARGO, https://www.wellsfargo.com/help/online-banking/advanced-access-faqs/ (last visited February 8, 2019) (defining Advanced Access as "a free service that gives you an additional layer of security to better protect your information and help prevent unauthorized transactions.").

64. *See Advanced Access Questions, supra* note 63 (requiring use of Advanced Access for "[sending] money to another person that you haven't transferred money to before, or receive money from a non-Wells Fargo account that you haven't used before.").

65. *How We Protect You, supra* note 62.

66. *How We Protect You, supra* note 62.

67. *How We Protect You, supra* note 62.

68. *See How We Protect You, supra* note 62 ("[O]utdated browsers could lead to a security risk.").

69. *See* Yalman Onaran, *Global Payment Firms Hold First Cyber War Game*, BLOOMBERG (October 12, 2018, 10:13 AM),

Mastercard, American Express, and others participated in exercises that unveiled crucial information about their varying approaches to defining what constitutes a "crisis."[70] The results of this exercise will be used to create a more streamlined system between these participating institutions, including an effort to efficiently communicate information about various threats.[71]

V. CONSUMER AND BANK REACTION TO SECURITY MEASURES

Banks and financial institutions are cognizant of how the security measures they enact impact customer satisfaction.[72] A survey conducted by Information Security Media Group discovered that 53% of financial institutions believe their customers view some of their security controls as inconvenient.[73] Moreover, 54% of institutions believe that they do a fair job balancing the priorities of responding to threats against cybersecurity and keeping the customer experience pleasant.[74] While banks appear to be moderately pleased with their ability to balance safety and consumer satisfaction, they are confident in their ability to defend a cyberthreat.[75] A study found that 78% of institutions have faith in their cybersecurity strategy as a whole.[76]

---

https://www.bloomberg.com/news/articles/2018-10-09/global-payment-firms-hold-first-cyber-war-game-to-test-readiness ("Global payment companies held their first joint cybersecurity war games to test their systems' readiness for simultaneous attacks, uncovering differences in their defenses including even how to define a crisis.").

70. *See id.* ("The participants discovered that they had varying definitions of a crisis related to breaches as well as differing approaches in how they reach out to law enforcement.").

71. *See id.* ("The sector will also seek a more formal way of sharing information on threats.").

72. *See* INFO. SEC. MEDIA GRP., PRESERVING THE CUSTOMER EXPERIENCE (2016) (stating that 63% of respondents say, when it comes to cybersecurity, that preserving a seamless customer experience is a top priority).

73. *See id.* ("[The survey] generated more than 150 responses from financial institutions primarily in the U.S., Canada, EMEA, Asia, and Australia. Respondent organizations all had 1,000 or more employees, and 30 percent manage assets of $20 billion or more.").

74. *See id.* (stating that they "say their organizations currently maintain a fair balance between cybersecurity and maintaining the online customer experience.").

75. Steve Evans, *Banks Confident About Cybersecurity, but Gaps Remain*, INFOSECURITY GROUP (March 9, 2017), https://www.infosecurity-magazine.com/news/banks-confident-about-cybersecurity/.

76. *See id.*; James Murphy, *Accenture Report: Banks Confident in Cybersecurity Capabilities But Lack of Real-World Testing Leaves Gaps in Their Defense,* ACCENTURE (April 19, 2017), https://newsroom.accenture.com/news/accenture-report-banks-confident-in-cybersecurity-capabilities-but-lack-of-real-world-testing-leaves-gaps-in-their-defense.htm (conducting the survey by polling "275 senior security executives across the banking and capital markets sectors").

When it comes to the customer experience, millions of Americans think security measures for phone and internet security are unduly burdensome.[77] A Fair, Isaac, and Company ("FICO") survey found that 81% of Americans find security measures "unnecessary".[78] Customers are undoubtedly relieved that their financial institution cares about protecting their information, but nonetheless are frustrated by how complicated the measures are when it comes to simply using their account.[79] Striking a delicate balance between security and customer experience will be key for institutions going forward.[80]

VI. THE FUTURE OF SECURITY AND A CALL FOR REGULATION

A. Regulatory Attempts and Failures

A development that has the potential for long-lasting impact is the presence of the Office of the Comptroller of the Currency ("OCC") Committee on Bank Supervision ("CBS").[81] In its Fiscal Year 2018 Operating Plan, CBS listed cybersecurity among its highest priority objectives for the year.[82] CBS called for an analysis of banks' and financial institutions' abilities to withstand cyberattacks.[83] A particularly

77. Scott Zoldi et al., *Survey: Americans are Frustrated by Security Measures*, FICO BLOG (July 9, 2018), http://www.fico.com/en/blogs/fraud-security/survey-americans-are-frustrated-by-security-processes/.

78. *See id.* (detailing that the survey was conducted by FICO and 72 Point, and polled 2,000 adults).

79. *Id.*

80. *See id.* (quoting TJ Horan, who oversees fraud solutions at FICO: "When it comes to digital transformation, a smooth customer experience is going to be vital. The winners will be the firms that can balance this against the need to stop fraud.").

81. OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC FISCAL YEAR 2018 BANK SUPERVISION OPERATING PLAN, https://www.occ.treas.gov/news-issuances/news-releases/2017/nr-occ-2017-113a.pdf (last visited Feb. 9, 2019) [hereinafter OCC FISCAL YEAR 2018 BANK SUPERVISION OPERATING PLAN]; Press Release by Bryan Hubbard, Office of the Comptroller of the Currency, OCC Releases Bank Supervision Operating Plan for Fiscal Year 2018 (September 28, 2017), https://www.occ.treas.gov/news-issuances/news-releases/2017/nr-occ-2017-113.html.

82. OCC FISCAL YEAR 2018 BANK SUPERVISION OPERATING PLAN, *supra* note 81, at 1.

83. *See id.* at 6 (calling for "assessing specific cybersecurity controls as part of information security, including key areas of cybersecurity risk management, such as the service providers' risk management, control structures, and level of cyber resilience. Examiners should assess banks' service providers' risk management structures for managing cybersecurity; assessing service providers' level of cyber resilience and completing the Federal Financial Institutions Examination Council's Technology Service Provider Cybersecurity Assessment Tool as part of the examination process.").

interesting portion of CBS' objective is their use of the FFIEC's CAT.[84] This illustrates how highly regarded CAT is for assessing an institution's cybersecurity protocol.[85]

For depository institutions, three of the main regulators are the OCC, the Federal Reserve Board ("FRB"), and the Federal Deposit Insurance Corporation ("FDIC").[86] The FRB is the federal regulator of state member banks, and the FDIC is the federal regulator for state non-member banks.[87] Moreover, the OCC is the chief regulator of national banks as well as federal savings associations.[88] Due to the important function they serve, one would reasonably believe that the OCC has strict, specific regulations that the banks they oversee must follow when it comes to protection of customers' data; however, this is not the case.[89] That is not to say that the OCC has been negligent or has turned a blind eye to this important issue.[90] In October 2016, the OCC, FRB, and FDIC promulgated a proposed regulation in regards to increased cybersecurity standards for organizations they supervised, which included all banks, savings associations, and savings banks.[91]

This proposed regulation would have only affected systematically important financial institutions ("SIFIs").[92] The proposed rule

---

84. *Id.*

85. *Id.* at 4.

86. LISSA L. BROOME & JERRY W. MARKHAM, REGULATION OF BANK FINANCIAL SERVICE ACTIVITIES 135 (5th ed. 2017).

87. *Id.*

88. OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC REGULATIONS, https://www.occ.treas.gov/topics/laws-regulations/occ-regulations/index-occ-regulations.html (last visited January 17, 2019) [hereinafter OCC REGULATIONS].

89. *See* OFFICE OF THE COMPTROLLER OF THE CURRENCY, FINAL ISSUANCES, https://www.occ.treas.gov/topics/laws-regulations/occ-regulations/final-issuances/index-final-issuances.html. (last visited January 17, 2019) [hereinafter FINAL ISSUANCES] (detailing how the OCC has promulgated numerous rules over the years, without any relating to cybersecurity).

90. FED. DEPOSIT INS. CORP., AGENCIES ISSUE ADVANCED NOTICE OF PROPOSED RULEMAKING ON ENHANCED CYBER RISK MANAGEMENT STANDARDS (October 19, 2016), https://www.fdic.gov/news/news/press/2016/pr16092.html.

91. Enhanced Cyber Risk Management Standards: A Proposed Rule by the Comptroller of the Currency, the Fed. Reserve System, and the Fed. Deposit Ins. Corp'n, 82 Fed. Reg. 8172 (proposed October 26, 2016) (to be codified at 12 C.F.R.pt. 364).

92. Shaun Waterman, *Business Lobby Pushes Back on Cyber Rule for Banks,* CYBERSCOOP (Jan. 19, 2017), https://www.cyberscoop.com/us-chamber-fdic-occ-federal-reserve-bank-cyber-rule/; *see also* Enhanced Cyber Risk Management Standards: A Proposed Rule by the Comptroller of the Currency, the Fed. Reserve System, and the Fed. Deposit Ins. Corp'n, 82 Fed. Reg. 8172 (proposed October 26, 2016) (to be codified at 12 C.F.R.pt. 364) (referring to those with more than $50 billion in assets, labeled systemically important by the Dodd-Frank financial reforms.).

narrowed their focus to SIFIs in that these are the institutions capable of having a large impact on the financial system in the event that a cyber-attack were to cripple one of these institutions.[93] The regulators allowed for an extended comment period in order to allow interested individuals an opportunity to let their voices be heard on this important and complicated topic.[94] However, a final rule was never promulgated once the comment period closed.[95] A common comment expressed concern about adding more regulation, instead proposing the centralization of existing regulations and the plugging of gaps in the regulatory framework instead.[96] Another concern focused on how an additional regulation would create an inflexible structure.[97]

The main reason a final rule never came to fruition can be traced to remarks made by the United States Chamber of Commerce.[98] In a letter sent to the OCC, the Board of Governors of the Federal Reserve, and the FDIC, the U.S. Chamber of Commerce expressed concern that strict requirements on banks and financial institutions would be unduly specific and would simply be a formulaic list of requirements.[99] The focal point of the Chamber of Commerce's letter was the formulaic list concern.[100] The letter concluded by stating, "[c]ybersecurity is not a one-size-fits-all proposition."[101] The Chamber of Commerce felt that organizations

93. *Id.*

94. Enhanced Cyber Risk Management Standards, 82 Fed. Reg. at 8172.

95. *See* FINAL ISSUANCES, *supra* note 89 (listing the final rules promulgated by the OCC, and not including "Enhanced Cyber Risk Management Standards.").

96. *See* THE CLEARING HOUSE ASS'N, COMMENT LETTER ON PROPOSED ENHANCED CYBER RISK MANAGEMENT STANDARDS 3 (Feb. 17, 2017), https://www.theclearinghouse.org//media/tch/documents/tchweekly/2017/20170217_comment_letter_enhanced_cyber_risk_management_standards.pdf ("The Clearing House accordingly recommends that, prior to proceeding with new requirements, the agencies should focus on consolidating existing standards, and work with industry stakeholders to assess the gaps that exist in the current regulatory framework….").

97. *See id.* ("Addressing the mechanism through prescriptive standards embeds inflexibility and a lack of responsiveness to new risks, which weakens institution-specific and sectoral risk management capabilities, and works at counter-purpose to our shared goals.").

98. U.S. CHAMBER OF COMMERCE, COMMENT LETTER ON PROPOSED ENHANCED CYBER RISK MANAGEMENT STANDARDS 6 (Jan. 18, 2017), https://www.uschamber.com/sites/default/files/documents/files/us_chamber_enhanced_standards_comment_letter_011817.pdf.

99. *Id.*

100. *Id.*

101. U.S. CHAMBER OF COMMERCE, *supra* note 98 at 6.

should be allowed to create a cybersecurity program based on their individual needs.[102]

State regulators are supplementing the efforts of federal regulators to fill the gaps they see in the regulatory structure.[103] The New York State Department of Financial Services ("DFS") unveiled its cybersecurity requirements for financial services companies in March 2017.[104] The DFS believed that new requirements were needed after finding that data breaches cost New York businesses upwards of $1.3 billion.[105] The DFS called for financial institutions to put measures in place, such as implementing a cybersecurity program and designating a Chief Information Security Officer[106] to protect customer information, and gave examples of acceptable security measures.[107] This scheme would have co-existed alongside the proposed rule that was never adopted, due to the fact that the NY scheme does not limit its scope specifically to SIFIs.[108]

B. Two Potential Courses of Action

Why should the onus be placed upon the banking and finance sector when breaches occur in virtually every industry?[109] Simply put, humans value money over most anything, and are likely to make changes

102. *See* U.S. CHAMBER OF COMMERCE, *supra* note 98 at 6 ("[C]ompanies must develop cybersecurity programs that are tailored to the risks that they face and their unique operational requirements.").

103. *See* NEW YORK STATE DEP'T OF FIN. SERVS., CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES (2017), https://blog.vasco.com/download/2416/ (codifying New York's cybersecurity regulations).

104. *Id.*

105. *See* Eric T. Schneiderman, N.Y. ATTORNEY GEN'S OFFICE, INFO. EXPOSED (July 14, 2014), https://ag.ny.gov/pdfs/data_breach_report071414.pdf (stating that the exact cost has been $1.37 billion).

106. *See* Waterman, *supra* note 92 (laying out the regulatory requirements).

107. *See* Michael Magrath, *Top Banking Regulations & Security Compliance Requirements for 2018,* ONESPAN, (August 29, 2018), https://blog.vasco.com/legal/top-banking-regulations-security-compliance-requirements-2018 ("Through a risk assessment, financial institutions must implement effective controls to prevent unauthorized access to information systems or non-public information. These controls may include multi-factor authentication, biometric authentication, or risk-based authentication.").

108. *See* NEW YORK STATE DEP'T OF FIN. SERVS., *supra* note 103 (stating that "Covered Entity" is defined as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.").

109. *See* IDENTITY THEFT RES. CTR., *supra* note 1, at 9 (detailing that breaches occurred in sectors including banking, business, education, government, and medical).

when their money may be compromised.[110] Therefore, since money is kept in the hands of banks and financial institutions, the pressure is ramped up on these entities.[111] Moreover, banks are of the utmost importance to our financial system as they take deposits from customers and then lend that money out to borrowers and attach an interest rate.[112] When banks fail, there is a massive ripple effect, best evidenced by the 2008 Financial Crisis in which twenty-five banks failed and closed, almost immediately, with many more following suit.[113]

The issue of cybersecurity for banks and financial institutions has become large enough that functional regulation should be considered as a viable option. Functional regulation is designed to make sure the "most qualified and knowledgeable people" are overseeing a particular field, such as banks or financial institutions.[114] The advantages of functional regulation include fairness and expertise.[115] The fairness advantage comes from the fact that all entities would be subject to the same cybersecurity regulations.[116]

110. *See* Suzanne Lucas, *Americans Value Money Over Time Off*, CBS MONEYWATCH (Feb. 28, 2014, 8:23 AM) https://www.cbsnews.com/news/americans-value-money-over-time-off/ ("Given a choice between an extra week of vacation or 5 percent increase in salary, 79 percent of Americans will take the raise, according to a recent survey by finance recruitment firm Accounting Principals."); *see also* Rahul Telang & Sriram Somanchi, *Security, Fraudulent Transactions, and Customer Loyalty: A Field Study*, CARNEGIE MELLON UNIVERSITY (Nov. 12, 2016, 12 AM), https://aisel.aisnet.org/icis2016/ISSecurity/Presentations/10/ ("[The study] focused on more than 500,000 customers of a leading U.S. bank over a five-year period and found that customers who experienced unauthorized charges on their account were one percentage point more likely than the average customer to end the relationship with their bank within the next six months.").

111. *See* Caroline Fairchild, *More Money Always Leads to More Happiness: Study*, HUFFINGTON POST (Apr. 29, 2013), https://www.huffingtonpost.com/2013/04/29/money-and-happiness-study_n_3179345.html (detailing that advances in income are always met with increases in life satisfaction).

112. *See The Business of Banking*, THE ECONOMIST (Oct. 28, 1999), https://www.economist.com/unknown/1999/10/28/the-business-of-banking ("[Banks] are vital to economic activity, because they reallocate money, or credit, from savers, who have a temporary surplus of it, to borrowers, who can make better use of it.").

113. *See* FED. DEPOSIT INS. CORP., BANK FAILURES IN BRIEF (Jan. 5, 2015), https://www.fdic.gov/bank/historical/bank/2008/index.html (briefly discussing the 25 banks across the United States that failed in 2008).

114. Will Kenton, *Functional Regulation*, INVESTOPEDIA, (May 21, 2018), https://www.investopedia.com/terms/f/functional-regulation.asp.

115. BROOME & MARKHAM, *supra* note 86, at 282.

116. *See* BROOME & MARKHAM, *supra* note 86, at 282 ("It is only fair that the same functions are regulated the same way, no matter what type of financial entity is performing the function.").

However, there are potential downsides to functional regulation.[117] Since this type of regulatory scheme divides regulatory authority based on type of product or service, there can be potential conflicts when innovation occurs and blends two defined services.[118] One example depicts how this blending can be problematic: derivatives created a disagreement between the CFTC and SEC over which entity had regulatory authority.[119]

In a functional regulatory scheme, a federal cybersecurity body should be created with the power and authority to enact uniform standards and regulations for the banking and financial industry. Creating a regulator that solely focuses on cybersecurity in the banking and finance industries would allow the regulator to become the "most qualified and knowledgeable" regulator due to having a singular focus.[120] The other major regulators in banking, e.g. the OCC, the FRB, and the FDIC, are responsible for regulating practically everything a bank does.[121] If these agencies attempt to regulate cybersecurity, in addition to the various complex issues they already oversee, this important issue likely will not receive the attention it deserves.[122]

---

117. *See* Patricia A. McCoy, BANKING LAW MANUAL: FEDERAL REGULATION OF FINANCIAL HOLDING COMPANIES, BANKS AND THRIFTS § 12.02 21 (2d ed. 2018) (discussing the several downsides of functional regulation).

118. *See id.* ("[B]ecause the functional approach divides regulatory authority according to established product lines, the regulatory apparatus has difficulty resolving jurisdictional quarrels over product innovations, particularly for new products that are hybrids of the old.").

119. *See id.* ("The SEC and the Commodities Futures Trading Commission dueled over who has jurisdiction over derivatives."); *see also* Dodd-Frank Wall Street Reform and Consumer Protection Act §§ 712, 717, 718, 722 12 U.S.C. § 5303 (2012) (2010)) (laying out the extent to which the SEC and CFTC each have authority over derivatives).

120. *See* Kenton, *supra* note 114 (stating that functional regulations will make sure that the "most qualified and knowledgeable people" are supervising a financial institution's activities).

121. *See* OCC REGULATIONS*, supra* note 88 (detailing the various regulations promulgated by the OCC as an example).

122. *See generally* Cesar Cerrudo, *Why Cybersecurity Should Be The Biggest Concern of 2017*, FORBES (Jan. 17, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/#698fb1135218 (discussing the vital importance of cybersecurity).

The problem with the current regulatory scheme is twofold.[123] First, there are many entities that are attempting to regulate.[124] This has led to regulations that conflict without one holding more weight than others.[125] Secondly, there is a tension between federal and state regulation of cybersecurity.[126] In addition to the aforementioned attempts by the NYCDFS and the OCC, regulations and rules have poured in from the Commodities Futures Trading Commission ("CFTC"), the National Credit Union Administration ("NCUA"), and the Financial Industry Regulatory Authority ("FINRA").[127] However, these regulators are only a subset of a much larger, murkier regulatory picture.[128] Other major regulators in play include the FRB and the FDIC.[129] An example is helpful to illustrate the illogical nature of this system: The Federal Trade Commission ("FTC") is not required to structure its penalties with the "best practices" put forward by the NIST.[130]

Moreover, the regulatory landscape is diluted due to the co-operative nature of state and federal cybersecurity laws.[131] By allowing a majority of states to implement data breach notification requirements-and a smaller subset of states attempting to get companies to follow guidelines to protect data-there is an abundance of regulation for companies and organizations that conduct business across the country.[132] This creates a culture of inefficiency for companies that operate in multiple states, as they must sort through potentially conflicting requirements. In practice, cybersecurity and cyber-attacks are a national, and in most cases, global

123. *See* Karen A. Popp & Edward R. McNicholas, *Regulatory Focus on Information Security Incidents,* BUS. & COMMERCIAL LITIG. IN FED. COURTS at 2 (Robert L. Haig, ed., 4th ed. 2017) (detailing the numerous parties that have promulgated cybersecurity regulations); *see also* Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985 (2018) (discussing the problems with current cybersecurity regulations).

124. *See* Popp & McNicholas, *supra* note 123 (detailing the numerous parties that have promulgated cybersecurity regulations).

125. *See* Popp & McNicholas*, supra* note 123 (discussing how the various parties that have issued cybersecurity regulations have led to conflicting law).

126. *See* Kosseff, *supra* note 123 (discussing the problems with current cybersecurity regulations).

127. Popp & McNicholas, *supra* note 123.

128. Popp & McNicholas, *supra* note 123.

129. *Federal Banking Regulators*, COMPLIANCE ALLIANCE, https://www.compliancealliance.com/laws-regulations/bank-regulators (last visited Jan. 26, 2019).

130. Kosseff*, supra* note 123, at 1029.

131. *See* Kosseff, *supra* note 123, at 1029 (discussing the problems with current cybersecurity regulations).

132. *See* Kosseff, *supra* note 123, at 1029 ("[I]t is difficult to align a set of effective cybersecurity incentives that apply to companies with national operations.").

threat.[133] It is not practical for states to exercise the control they currently do, as this is an area that calls for strong leadership from the federal government.[134] New York wanted to create a culture of regulatory compliance when they passed new regulations in 2017, and this federal regulatory body is poised to accomplish the same goal in a more uniform, centralized manner.[135]

Creating a new regulatory body would eliminate the need for all of the existing regulations that have been promulgated across different regulatory bodies.[136] The biggest potential benefit of having a new regulator would be the possibility of an increase in consumer confidence about the protection of their data. Consumers would see that the federal government is taking cybersecurity issues seriously, rather than letting numerous agencies create rules and guidance on the issue.

An important practical point when it comes to this idea is the current political climate in the U.S.[137] The idea of fewer regulations fits within the Trump Administration's theme of deregulation.[138] In May 2018, President Trump signed the Economic Growth, Regulatory Relief, and Consumer Protection Act, putting into place the "biggest rollback of financial regulation since the Dodd-Frank Act."[139] Creating a new federal regulatory body falls in line with President Trump's mission in that doing so would allow the existing rules and regulations to be removed and then replaced by one institution.[140] The cumulative effect of rolling back the existing regulations and replacing them with new regulations promulgated by a federal body should-ideally-result in a net decrease in

133. *See Kosseff*, *supra* note 123, at 1029 (discussing how cybersecurity threats are "inherently interstate (and global)" in nature).

134. *See* Kosseff, *supra* note 123, at 1029 (discussing whether it is "practical—for states to continue to exercise such control over the future of U.S. cybersecurity law.").

135. *See* Sabrina Galli, Note, *NYDFS Cybersecurity Regulations: A Blueprint for Uniform State Statute?*, 22 N.C. BANKING INST. 235, 236 (2018) ("NYDFS' new regulations place a tremendous amount of responsibility on financial institutions and shift the business strategy from a mindset of risk mitigation to one of regulatory compliance.").

136. *See* Popp & McNicholas, *supra* note 123 (discussing the various bodies that have promulgated regulations on the issue of cybersecurity).

137. *See* Terry Jones, *Deregulation Nation: President Trump Cuts Regulations at Record Rate,* INVESTORS (August 14, 2018), https://www.investors.com/politics/commentary/deregulation-nation-president-trump-cuts-regulations-at-record-rate/ (discussing a policy goal of the Trump Administration).

138. *See id.* (arguing that de-regulation is a focal point of the Trump Administration).

139. Elizabeth Dexheimer, *Trump Signs Biggest RollBack of Bank Rules Since Dodd-Frank Act,* BLOOMBERG (May 24, 2018, 12:20 PM), https://www.bloomberg.com/news/articles/2018-05-24/trump-signs-biggest-rollback-of-bank-rules-since-dodd-frank-act.

140. Jones, s*upra* note 137.

number of regulations.[141] Under this scheme, state regulations should be preempted by the federal regulations, as the state regulations that were designed to "plug gaps" will no longer be necessary.

A legitimate concern about this proposed course of action centers around how a new regulator would be funded. The most logical funding scheme would involve an examination fee being charged to each financial institution. With the average cost of a breach hovering around $4 million, notwithstanding additional costs such as loss of business, financial institutions should see the benefit of spending a small sum in the short-run in order to save a large amount of money in the long-run.[142]

In the event that it is deemed too burdensome to create a new federal agency, or that regulation will not be able to keep up with novel scammer tactics, all regulators of the financial industry should be required to examine institutions based on CAT results. This possibility will also shift the approach from punishing institutions that do not meet regulatory requirements to a system that focuses on helping banks avoid cyber-attacks.[143] One issue that makes this difficult is that some regulators have determined that use of CAT is not required.[144] For example, the FDIC, OCC, and FRB all have stated that use of CAT is optional.[145]

While all institutions are encouraged to use CAT to assess their own maturity levels-and in fact many institutions have completed CAT assessments-it is natural that some smaller institutions may not have the

141. Jones, *supra* note 137.

142. *See* Grillo, *supra* note 30 ("The average dollar cost of a breach is reported to be $4 million, yet regulated industries, such as health care and financial services, pay a higher price because of fines and the higher-than-average rate of lost business and customers.").

143. *See* FED. FIN. INST. EXAMINATION COUNCIL, CYBERSECURITY ASSESSMENT TOOL, https://www.ffiec.gov/cyberassessmenttool.htm (last visited February 8, 2019) (explaining that CAT will "help institutions identify their risks and determine their cybersecurity preparedness" because "[t]he Assessment provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time.").

144. Tom Hinkel, *Cybersecurity and Compliance: What You Need to Know*, BANK NEWS, https://www.banknews.com/blog/cybersecurity-and-compliance-what-you-need-to-know/ (last visited Jan. 29, 2019).

145. *See* FED. DEPOSIT INS. CORP., CYBERSECURITY ASSESSMENT TOOL (July 2, 2015), https://www.fdic.gov/news/news/financial/2015/fil15028.html ("Use of the Cybersecurity Assessment Tool is voluntary."); *see also* OFFICE OF THE COMPTROLLER OF THE CURRENCY, FFIEC CYBERSECURITY ASSESSMENT TOOL (June 30, 2015), https://www.occ.gov/news-issuances/bulletins/2015/bulletin-2015-31.html ("While use of the Assessment is optional for financial institutions, OCC examiners will use the Assessment to supplement exam work to gain a more complete understanding of an institution's inherent risk, risk management practices, and controls related to cybersecurity.").

infrastructure to conduct this voluntary review.[146] This likely explains why these three regulators make CAT use optional, as they do not want to unduly burden smaller institutions.[147] However, regulators still expect smaller institutions to have infrastructure in place to keep track of cyber threats and attacks.[148] The difference is that rather than force these smaller institutions to use CAT, which is time-consuming,[149] they are allowed to seek out other alternatives, such as hiring an IT service provider.[150]

CAT assessment completion is not the end of the road; a crucial following step is to conduct a "gap analysis."[151] This informs the institution of the measures necessary to bring the institution's results into accordance with a desired level by either minimizing risk or enhancing maturity.[152] The desired level is contingent on the amount of risk the institution's board of directors is willing to tolerate, and thus different for almost every institution.[153] After a risk tolerance is established by the Board, the institution can establish whether the outstanding risks are within the amount of tolerance accepted by the board.[154]

While requiring regulators to examine based on CAT results will be an important first step, the examination will be fruitless without appropriate enforcement tools to use if CAT performance is deemed inadequate by the regulator. For example, the OCC has a variety of enforcement tools at its disposal, ranging from commitment letters and formal

146. *See* Hinkel, *supra* note 144 ("[T]hreat intelligence and collaboration can be a challenge for smaller financial institutions that don't have dedicated cybersecurity resources.").

147. Hinkel, *supra* note 144.

148. *See* Hinkel, *supra* note 144 ("Even though your community bank may lack the size and complexity of the larger national banks, regulators still expect all financial institutions to identify and monitor cyber threats, and to use that information to inform their own risk environment as well as their specific controls.").

149. *See* Hinkel, *supra* note 144 ("The CAT assessment itself is 123 pages, with 69 questions and 10 categories.").

150. *See* Hinkel, *supra* note 144 (stating that another option for cybersecurity, other than performing a CAT, is "utilizing a local IT service provider").

151. *See* Hinkel, *supra* note 144 ("Once your bank has completed both sections of the CAT, management should perform a gap analysis to determine the next steps.").

152. *See* Hinkel, *supra* note 144 ("The gap analysis should rank in importance the actions needed to reduce risks or increase control maturity in order to bring the actual state of operations in line with the desired state.").

153. *See* Hinkel, *supra* note 144 ("The desired state should be based on an official risk appetite approved by the board.").

154. *See* Hinkel, *supra* note 144 (stating how once banks settle on a risk tolerance, they can evaluate whether their current risks are at a level that fits into their risk tolerance).

agreements to civil money penalties.[155] These tools will need to be used by the OCC to bring financial institutions into accordance with adequate standards.[156] The FDIC states that they will communicate with the institution they are examining about CAT in order to ensure awareness of the tool, but this is not enough.[157] Simply putting an institution on notice about CAT will not make a difference; the institutions that are not up to an appropriate standard based on the findings of CAT will need to be informed of their deficiency. Moreover, the FDIC needs defined enforcement tools in place specifically designed to handle issues regarding CAT.[158]

By requiring that regulators examine institution's using CAT results, financial institutions will be forced to come face-to-face with their cybersecurity issues.[159] Most institutions have already acknowledged the major threat that a cyber-attack poses.[160] For the institutions whose CAT results are problematic, the regulator will be able to better point out these deficiencies, ideally allowing the institution to rapidly fix their problems.

At the end of the day, banks and financial institutions should make it a fundamental goal to reach a high level of cyber-resilience.[161] These institutions should shift the focus from a system of attempting to simply comply with applicable regulations to one of effective

155. *See* OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC ENFORCEMENT ACTION POLICIES AND PROCEDURES MANUALS, (Nov. 13, 2018), https://www.occ.treas.gov/news-issuances/bulletins/2018/bulletin-2018-41.html (laying out the various informal and formal enforcement mechanisms at the OCC's disposal).

156. *See id.* (setting forth the various informal and formal enforcement mechanisms at the OCC's disposal).

157. *See* FED. DEPOSIT INS. CORP., *supra* note 145 ("FDIC examiners will discuss the Cybersecurity Assessment Tool with institution management during examinations to ensure awareness and assist with answers to any questions.").

158. *See* FED. DEPOSIT INS. CORP., FDIC ENFORCEMENT DECISIONS AND ORDERS (September 4, 2018), https://www5.fdic.gov/EDO/index.html (explaining that the FDIC can initiate "enforcement actions…. for violations of laws, rules, or regulations, unsafe or unsound banking practices, breaches of fiduciary duty, and violations of final orders, conditions imposed in writing or written agreements.").

159. *See* OFFICE OF THE COMPTROLLER OF THE CURRENCY, *supra* note 145 ("While use of the Assessment is optional for financial institutions, OCC examiners will use the Assessment to supplement exam work to gain a more complete understanding of an institution's inherent risk, risk management practices, and controls related to cybersecurity.").

160. *See* Grillo, *supra* note 30 ("Companies in North America view cybercrime and hacking as their No. 1 risk.").

161. *See* Grillo, *supra* note 30 ("Ultimately, cyberresilience—the ability to defend, respond to, and recover from a breach—is the end goal for financial institutions, which tend to be facing thousands of attacks every day.").

cybersecurity due diligence.[162] Mandating the completion of CAT, combined with regulators having appropriate enforcement tools if institutions' CAT results are found to be inadequate, is a central first-step towards achieving cyberresilience.[163]

VII. CONCLUSION

Cybersecurity and protection of consumer data is a major issue facing the world today.[164] Banks and financial institutions should be aware that consumers may sever ties with their respective bank after a data breach occurs.[165] The call for uniform federal cybersecurity regulation is one that could have long-lasting effects for the banking and financial industry. One potential explanation for the high number of breaches that occur today is the lack of uniform standards employed by various institutions.[166] If every institution were monitored and required to employ at least a minimum baseline of protection, hackers would not be able to take advantage of institutions with suboptimal security requirements.[167]

Regardless of which method is used, it is clear that federal action is required on this issue.[168] Consumers need to feel that their representatives have the same degree of urgency about this issue as they do. The OCC's inclusion of cybersecurity among its main objectives for this fiscal year is a step in the right direction[169], but in order for meaningful change to take place, consumers need a regulatory body with the ability to touch a wide variety of institutions to develop regulations and rules in a uniform manner.[170] If swift action is not taken, the damage to sensitive information could be devastating.

---

162. *See* Grillo, *supra* note 30 ("The focus should be shifted toward conducting good cyber due diligence and assessments.").

163. *See* Grillo, *supra* note 30 (discussing cyberresilience).

164. *See supra* Part I (discussing the data breaches that have occurred).

165. *See supra* Part III (detailing consumer reactions to data breaches).

166. *See* IDENTITY THEFT RES. CTR., *supra* note 1 (discussing the high number of breaches that have taken place).

167. *See* James A. Lewis, *Raising the Bar for Cybersecurity*, CTR FOR STRATEGIC & INT'L STUDIES (Feb. 12, 2013), csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf ("96% of successful breaches could have been avoided if the victim had put in place simple or intermediate controls.").

168. *See supra* Part VI (discussing two options for change).

169. OCC FISCAL YEAR 2018 BANK SUPERVISION OPERATING PLAN, *supra* note 81.

170. *See supra* Part VI (discussing the need for uniform federal cybersecurity regulation for the financial industry).

ZACHARY N. LAYNE*

*I would like to thank Professor Broome, as well as my editors, Katie Clarke and Stephen Spivey, for all of their feedback and guidance throughout this process. Also, thank you to my amazing parents, brother, and Zoe for always supporting me throughout my academic career.