Bank Disclosures of Cyber Exposure

Christina Parajon Skinner[*]

ABSTRACT: Financial institutions are increasingly subject to cyber incidents and attacks. Cyber intrusions threaten these institutions' balance-sheets and reputations, and can undermine their resilience. From a societal perspective, cyber risk is particularly concerning as it regards systemically important financial institutions, like the largest internationally active banks. This is because the stability of the financial system as a whole—and thus the real economy—depends on these banks' resilience to stressful events, including cyber attacks. To date, the SEC has taken the lead among the financial regulators in addressing cyber risk, chiefly through an emphasis on disclosure. This Article critically examines the existing design of that mandatory disclosure regime by reviewing the content of nearly 900 SEC filings made by the seven systemically important U.S. bank holding companies over a three-year period. That review suggests that the current trajectory of SEC rules and guidance is in some ways overbroad as applied to these institutions; but in other ways, the rules and guidance remain inadequate to address the various public and private interests at stake. The Article urges the SEC to design a more nuanced set of rules for cyber disclosure, which would be better tailored for systemically important banks.

[*] Assistant Professor, Legal Studies and Business Ethics, The Wharton School of the University of Pennsylvania. With thanks to Brian Feinstein, Merritt Fox, Zohar Goshen, Paul Mahoney, Henry Monaghan, Frank Partnoy, Bob Thompson, and workshop participants at IU Maurer School of Law and Minnesota Law School, for generous feedback on drafts of this Article. Megan York provided excellent research assistance.

I. INTRODUCTION

Cyber intrusions are one of the most pressing risks facing financial institutions today.[1] Cyber risk presents corporate governance challenges for these institutions to manage, as well as financial stability threats for the bank regulator to address. Because banks provide critical services to the broader economy, such as payments, credit, and demand deposits, a large bank's vulnerability to a cyber attack—which could threaten the disruption of these critical services—presents the potential for adverse spillover effects. Indeed, precisely as Kevin Stiroh, the New York Fed's Executive Vice President of the Financial Institution Supervision Group, remarked in April 2019, "You don't need to convince anyone that this is a fundamental risk for financial firms, the financial system, and the broader economy."[2] Cyber risk would thus seem to present a classic case for regulatory intervention.[3] But how should such regulation be designed?

Among the various financial regulators, the Securities and Exchange Commission ("SEC") has been particularly attentive to cyber risk. While banking law and regulation has remained relatively inert in the face of

1. According to an annual data breach investigation report published by Verizon in concert with 67 other national and economic security organizations, of the 64,199 cyber incidents that they studied, about 1,368 of the incidences and 795 of the confirmed breaches occurred in the financial services industry. Penny Crosman, *Where Banks Are Most Vulnerable to Cyberattacks Now*, AM. BANKER (Apr. 26, 2016, 12:00 PM), https://www.americanbanker.com/news/where-banks-are-most-vulnerable-to-cyberattacks-now [https://perma.cc/DGS9-TY25].

2. *See* Kevin Stiroh, Exec. Vice President, Fed. Reserve Bank of N.Y., Thoughts on Cybersecurity from a Supervisory Perspective at the SIPA's Cyber Risk to Financial Stability: State-of-the-Field Conference 2019 (Apr. 12, 2019), *available at* https://www.bis.org/review/r190430l.pdf [https://perma.cc/CLN2-E94Q].

3. A recent White House report on the issue relied on such economic justification for regulatory intervention in cyber risk: "Importantly, cyberattacks and cyber theft impose externalities that may lead to rational underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment." EXEC. OFFICE OF THE PRESIDENT, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 1 (2018), *available at* https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf [https://perma.cc/CW89-J6ZX] [hereinafter WHITE HOUSE REPORT].

mounting cyber risk, the SEC has taken several steps forward. In February 2018, the SEC expanded and augmented a piece of regulatory guidance which was first issued in 2011. In that guidance, SEC Chairman Jay Clayton made clear that "[p]ublic companies must stay focused on [cybersecurity] issues and take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion."[4] That 2018 guidance explained that firms are obligated by the Securities Act of 1933 and Securities Exchange Act of 1934 to disclose their cyber controls, risks, and vulnerabilities.[5] This Article questions whether the sharpening of mandatory disclosure requirements—through sub-regulatory guidance no less[6]—is justified in the particular case of systemically important banks.

To be sure, the SEC has legitimate reason to be concerned about under-disclosure of cyber risk by public companies generally. Many seem to be dragging their feet in disclosing major breaches. Equifax, for example, waited months to disclose the fact that it had suffered a "cybersecurity incident" of unprecedented scale in the spring-summer of 2017—a breach that affected 143 million Americans.[7] Similarly, Yahoo! waited nearly two years to disclose a massive cyber incident from 2014.[8]

---

4. Jay Clayton, Chairman, SEC, Statement on Cybersecurity Interpretive Guidance (Feb. 21, 2018), *available at* https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21 [https://perma.cc/RQR8-L8XF]; *see also Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, SEC (Feb. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf [https://perma.cc/PL5D-58ZP] [hereinafter *SEC Cyber Guidance*].

5. The SEC has also created a separate cyber unit. Press Release, SEC, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors (Sept. 25, 2017), *available at* https://www.sec.gov/news/press-release/2017-176 [https://perma.cc/Z2HT-XAH3]; *see also* Jonathan S. Kolodner et al., *Cleary Gottlieb Discusses the SEC's New Cyber Unit, Six Months On*, COLUM. L. SCH.: CLS BLUE SKY BLOG (Apr. 3, 2018), http://clsbluesky.law.columbia.edu/2018/04/03/cleary-gottlieb-discusses-the-secs-new-cyber-unit-six-months-on [https://perma.cc/3WBX-9K45] (noting that cyber related disclosure has also been identified as an "enforcement interest" for the Cyber Unit).

6. Sub-regulatory guidance is not open to public comment in the way that formal rulemaking is. As Deputy Associate Attorney General Claire McCusker Murray noted, "subregulatory guidance isn't law—it's just paper." Still, subregulatory guidance greatly impacts the application of a law on the ground and companies may perceive it as a signal of the regulator's priorities—and, in turn, its enforcement priorities. Claire McCusker Murray, Deputy Assoc. Att'y Gen., DOJ, Remarks at the Compliance Week Annual Conference (May 20, 2019), *available at* https://www.justice.gov/opa/speech/remarks-principal-deputy-associate-attorney-general-claire-mccusker-murray-compliance [https://perma.cc/GRU6-2FML]; *see also* Nicholas R. Parrillo, *Federal Agency Guidance and the Power to Bind: An Empirical Study of Agencies and Industries*, 36 YALE J. ON REG. 165, 171 (2019).

7. *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 [https://perma.cc/JSN3-8398].

8. *In re* Altaba Inc, Yahoo! Inc., Order Instituting Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933 and Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Case-and-Desist Order, SEC Release No. 3,937 Securities Act, Release No. 10,485, Securities Exchange Act Release No. 83,096, 2018 WL 1919547 (Apr. 24, 2018).

In light of these delays, it could be appropriate to press certain nonfinancial public companies for more timely disclosure of their cyber incidents. After all, classic disclosure law theory maintains that fulsome public company disclosure enables market (i.e., price) efficiency—by that theory, the timely disclosure of cyber breaches would allow the price of those companies' shares to reflect the company's value as discounted by its shortcomings in managing cyber risk.[9] Disclosure should also, in theory, better equip a company's debt and equity investors to hold managers and board members accountable for adequate cyber risk management.[10]

But systemically important banks may present a special case. Publicizing the details of a bank's cyber vulnerability can further weaken that bank, which can lead to macro instability. News of a cyber breach at a large bank could, for instance, instigate depositor panic, thereby precipitating a plunge in the perceived value of a bank's assets. Such disclosure could also flag open wounds to would-be cyber attackers, inviting more intrusions. As such, pressing very large *banks* to disclosure more information about their cyber issues could work at cross-purposes to certain financial stability goals of banking regulation, even if such disclosure could improve market efficiency.

Arguably, the SEC should weigh and balance the various interests in market efficiency on the one hand, with resilience and financial stability on the other. On that view, the core claim of the Article is that the SEC's current approach to cyber disclosure has given short shrift to this kind of weighting and balancing analysis, and further refinement along those lines would lead to a more optimally designed disclosure regime. As such, the primary goal of the Article is to prompt renewed consideration of what kind of cyber disclosure the SEC should require from systemically important banks.

To do this, the Article collects and examines data about what exactly the systemically important U.S. banks have been disclosing about their exposure to cyber risk. Specifically, I hand-collected a set of three types of SEC filings over a three-year span, which were filed by the seven U.S. bank holding companies that have been designated as global systemically important financial institutions by the Financial Stability Board: JP Morgan, Bank of America, Citigroup, Wells Fargo, Goldman Sachs, BNY Mellon, and Morgan Stanley.[11] I reviewed all of these banks' SEC-filed 8-K forms (which disclose 'material' current events), 10-K forms (which are a company's annual

9. Zohar Goshen & Gideon Parchomovsky, *On Insider Trading, Markets, and "Negative" Property Rights in Information*, 87 VA. L. REV. 1229, 1233 (2001) (discussing literature on the link between information and insider trading); Yesha Yadav, *How Algorithmic Trading Undermines Efficiency in Capital Markets*, 68 VAND. L. REV. 1607, 1612 (2015); *see, e.g.*, John C. Coffee, Jr., *Market Failure and the Economic Case for a Mandatory Disclosure System*, 70 VA. L. REV. 717, 722–24 (1984) (discussing the relevance of information for mandatory disclosure).

10. *See, e.g.*, Lucian Arye Bebchuk, *The Case for Increasing Shareholder Power*, 118 HARV. L. REV. 833, 850–53 (2005) (discussing agency cost theory rationale for mandatory disclosure).

11. This set of institutions comprises all of the U.S. Bank Holding Companies that were designated as globally systemically important banks at the time this Article was drafted.

statement to the SEC and shareholders), and proxy statements (which announce shareholder meetings, items on the agenda, and other important governance related information). The filings span fiscal years 2016 to 2018. I then searched and reviewed each document for any references to "cyber" —ranging from benign references to enumerated committee oversight duties to, in theory, any disclosure of actual or imminent cyber threat.

On a high-level, my review of nearly 900 SEC filings yielded results that were generally consistent with other studies on the subject: Banks, like other public companies, are not disclosing very much about their exposure to cyber risk.[12] In particular, the banks studied here never disclose actual cyber breaches in the relevant SEC Form 8-K.

There are two possible interpretations of this data, which lead to two different policy conclusions. On the one hand, this data could suggest that banks are under-disclosing their cyber issues. On that analysis, a policymaker would likely conclude that the SEC should continue to press for more disclosure because "events like these matter to the market."[13] This more or less reflects the SEC's current regulatory stance. The SEC's recent guidance on the subject urges all public companies (not only banks) to be more robust in disclosing cyber issues across the range of their periodic filings, material event-based filings, and proxy materials.[14] On the other hand, some might find the current status of bank disclosures wholly satisfying, on the view that further disclosures would threaten to undermine banks' ongoing efforts to shore up their cyber defenses and, in any case, disclosing cyber breaches is merely a tail that wags the dog.

But there is an important middle ground which this Article espouses. That is, the data presented here also suggest that cyber disclosure requirements—particularly for systemically important banks—can and should be more finely tuned, and in some cases, more judicious. More specifically, the Article demonstrates that a simple tally of the disclosures does not present a complete picture. Studying the content of the disclosures reveals that while these large banks do not disclose cyber events, they do disclose other types of cyber issues relating to their internal processes and controls, and their investment in mitigating cyber risk. The banks also provide some predictive —and sobering—discussion of the magnitude of risk facing their businesses and the way they view cyber risk on the horizon. On a more negative note, this content-based study also reveals that most of the banks' cyber disclosures remain too general to be useful for benchmarking their cyber risk management efforts against each other or gaining a firm sense of how well the banks' procedures and controls are working to mitigate their cyber risk.

---

12. *See, e.g.*, Robert J. Jackson, Jr., Comm'r, SEC, *Corporate Governance: On the Front Lines of America's Cyber War* (Mar. 15, 2018), https://www.sec.gov/news/speech/speech-jackson-cybersecurity-2018-03-15 [https://perma.cc/77Y2-MBD2].

13. *Id.*

14. *SEC Cyber Guidance*, *supra* note 4.

Drawing insight from the content of these disclosures, the Article suggests that the SEC would be justified in pressing banks to disclose more detail surrounding their controls, processes, and investments in cyber risk management, but advises the SEC to take the pressure off banks to disclose cyber events via the Form 8-K. The data presented here also points to areas where the financial stability regulator (e.g., the Federal Reserve) should step in: that is, to prevent macro financial stability risk associated with the cyber risk.

The Article proceeds as follows. Part II provides doctrinal background on how financial regulation and corporate governance view cyber risk—that is, as an "operational risk" to the bank's business. It also sets forth the existing landscape of disclosure law relevant to operational (which now includes cyber) risk.

Parts III and IV generate a framework for analysis which could be used for fine-tuning bank cyber disclosure rules going forward. The first step, the Article argues, is to reflect on how much and what banks are disclosing about their cyber issues. As such, Part III discusses the content of the banks' cyber disclosures and develops a novel typology of cyber disclosures. That typology identifies and categorizes disclosure into three categories: "negative/risk"; "organizational/neutral"; and "preventative/investment" disclosures.

Part IV interprets this data further with a market failure analysis. The aim here is to gauge the costs and benefits of requiring banks to disclose different types of cyber information, as an approach to discerning a more optimal design. By examining how well a particular type of cyber disclosure addresses the various interests at stake—market efficiency, board and management accountability, and financial stability—Part IV suggests that requiring more disclosure of prevention, organizational, and investment related cyber information may be justifiable, while the costs of requiring more event-based disclosure may outweigh the gains.

Part V of the Article briefly considers the limits of disclosure in addressing the core financial stability risk at stake. Disclosure, after all, is not a tool specifically designed to prevent systemic cyber risk. For that, different kinds of tools are needed. Part V therefore draws on some implications of the data to contribute a new perspective to the ongoing policy and academic conversations about macro financial stability regulation—macroprudential regulation, as it is called.[15] Ultimately, then, this Article joins a classic corporate governance analysis with a contemporary financial stability one.

---

15. Ben S. Bernanke, Chairman, Bd. of Governors of the Fed. Reserve Sys., Remarks on Implementing a Macroprudential Approach to Supervision and Regulation at the 47th Annual Conference on Bank Structure and Competition (May 5, 2011), *available at* http://www.federalreserve.gov/newsevents/speech/bernanke20110505a.pdf [https://perma.cc/ENgJ-DAHR] (explaining this approach as one "that supplements traditional supervision and regulation of individual firms or markets with explicit consideration of threats to the stability of the financial system as a whole"); *see, e.g.*, JOHN ARMOUR ET AL., PRINCIPLES OF FINANCIAL

II. CYBER RISK AS OPERATIONAL RISK

For banks, cyber risk is considered an "operational risk" to the business. The Basel Committee on Banking Supervision—the international regulatory networking committee comprised of national bank regulators—has long defined operational risk "as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk."[16] In that vein, the big banks have traditionally considered the universe of operational risks to include various forms of systems failures, physical events (like natural disasters), or isolated instances of employee fraud or malfeasance.[17] Operational risk has also been used as a catchall risk bucket, for other "external events."[18]

For the most part, operational risk was (for the bulk of its acknowledged existence) treated as secondary in importance to the seemingly more salient risks to the bank's balance sheet, like credit or liquidity risk.[19] The advent of serious cyber risk has changed this state-of-play. Cyber risk is now included under the operational risk heading, as a kind of risk to financial institutions' information and data security.[20] Adding cyber to the operational risk category

---

REGULATION 425 (2016) ("One of the most important post-crisis financial regulatory reforms has been the creation of new MPAs [macroprudential authorities], charged with identifying systemic risk and invoking or coordinating various macroprudential tools.").

16. *See* BASEL COMM. ON BANKING SUPERVISION, PRINCIPLES FOR THE SOUND MANAGEMENT OF OPERATIONAL RISK 3 n.5 (2011) [hereinafter BASEL, SOUND MANAGEMENT]. The Basel Committee first began to discuss operational risk in 2003 with the publication of *Sound Practices for the Management and Supervision of Operational Risk*.

17. *See* Bank of Am. Co., Current Report (Form 8-K) 78 (Nov. 1, 2016); Citigroup Inc., Annual Report (Form 10-K) 117 (Feb. 23, 2018) (noting that in this document, CitiGroup refers to "inadequate or failed . . . systems or human" factors); JP MORGAN CHASE & CO, ANNUAL REPORT 75 (2018), *available at* https://www.jpmorganchase.com/corporate/investor-relations/document/annualreport-2017.pdf [https://perma.cc/LQL9-VKRY] [hereinafter JP MORGAN 2017 ANNUAL REPORT]; Wells Fargo, Quarterly Report (Form 10-Q) 29 (Nov. 6, 2018) [hereinafter Wells Fargo, Form 10-Q, Q3 2018]; *see also* BASEL, SOUND MANAGEMENT, *supra* note 16, at 1.

18. BASEL, SOUND MANAGEMENT, *supra* note 16, at 3 n.5.

19. Credit risk can be understood as follows, in the words of Wells Fargo: "When we loan money or commit to loan money we incur credit risk, or the risk of losses if our borrowers do not repay their loans. As one of the largest lenders in the U.S., the credit performance of our loan portfolios significantly affects our financial results and condition." WELLS FARGO, 2017 ANNUAL REPORT TO SHAREHOLDERS 129 (2018), *available at* https://wwwo8.wellsfargomedia.com/assets/pdf/about/investor-relations/annual-reports/2017-annual-report.pdf [https://perma.cc/C554-8XJN] [hereinafter WELLS FARGO 2017 ANNUAL REPORT]. Meanwhile, "The primary role of liquidity-risk management is to (1) prospectively assess the need for funds to meet obligations and (2) ensure the availability of cash or collateral to fulfill those needs at the appropriate time by coordinating the various sources of funds available to the institution under normal and stressed conditions." *Supervisory Policy and Guidance Topics: Liquidity Risk Management*, BOARD GOVERNORS FED. RES. SYS., https://www.federalreserve.gov/supervisionreg/topics/liquidity_risk.htm [https://perma.cc/43B7-MLCN].

20. *See, e.g.*, BASEL COMM. ON BANKING SUPERVISION, CYBER-RESILIENCE: RANGE OF PRACTICES 9 (2018) [hereinafter BASEL, CYBER-RESILIENCE]; *see also infra* notes 25–28 and accompanying text.

has no doubt elevated the importance of operational risk to some bank supervisors and regulators.[21] Yet the direct regulation of operational risk in banks has remained largely unchanged. Meanwhile, the securities regulator —the SEC—has taken a lead in trying to address cyber risk through the mandatory disclosure regime that applies to all public companies.

This Part provides the necessary context for understanding how disclosure is used as a tool for addressing the market failures that cyber risk in banks poses. Accordingly, Part II first discusses some basic principles of how banks manage operational risk, and cyber risk specifically. Part II then explains the existing disclosure requirements that are relevant to operational risk and, in particular, how the SEC has attempted to carve out a bespoke framework for cyber risk through the issuance of sub-regulatory guidance.

A. CORPORATE GOVERNANCE AND OPERATIONAL RISK

Managing and overseeing risk is one of the primary responsibilities of bank managers and boards. While banks have always had to manage risks, the events of the 2008 global financial crisis shined a light on the importance of risk management in banks.[22] Under post-crisis regulatory scrutiny, many large banks revisited and revamped their risk management processes or procedures—yet the bulk of these reforms focused on the management of credit and liquidity risk as the main culprits of the financial crisis.[23] The influx of cyber intrusions and attacks on banks has again forced these institutions to revisit their internal processes for risk management; now, with a view to managing cyber risk as a distinct kind of operational risk. Indeed, as SEC Commissioner Robert Jackson has emphasized, "the rising cyber threat" "is the most pressing issue in corporate governance today."[24]

Citigroup and Wells Fargo, for example, have already begun to call out cyber risk specifically under the heading of operational risk, and it is almost certain the other banks will follow suit. For example, in its 2017 Annual Report, Wells Fargo notes that "[i]nformation security is a significant operational risk for financial institutions such as Wells Fargo, and includes

---

21. *See* Piotr Kaminski et al., *Nonfinancial Risk: A Growing Challenge for the Bank*, MCKINSEY & CO. (July 2016), https://www.mckinsey.com/business-functions/risk/our-insights/nonfinancial-risk-a-growing-challenge-for-the-bank [https://perma.cc/MPV3-9RCU] ("Despite recent improvements, many bank boards do not routinely consider [nonfinancial risk] management, engaging only in some firefighting when risk controls fail."). Tellingly, operational risk is generally listed as the last or penultimate risk under Item 1A of the Form 10-K. As the SEC notes, "[c]ompanies generally list the risk factors in order of their importance." *Fast Answers: How to Read a 10-K*, SEC, https://www.sec.gov/fast-answers/answersreada10khtm.html [https://perma.cc/UNM2-Z7XH].

22. *See generally* FIN. CRISIS INQUIRY COMM., FINANCIAL CRISIS INQUIRY REPORT (2011) (recognizing the general consensus that the failure to prudently manage risk related to the banks' exposure to mortgage products was thought to be a key contributor to that crisis).

23. *Id.*

24. Jackson, *supra* note 12.

the risk of losses resulting from cyber attacks."[25] While Citigroup did not make explicit the fact that cyber risk fell under the operational risk umbrella in 2017, in its most recent 2018 10-K filing, it dedicates a specific sub-category discussion to cyber risk: "Cybersecurity risk is the business risk associated with the threat posed by a cyber attack, cyber breach or the failure to protect Citi's most vital business information assets or operations, resulting in a financial or reputational loss."[26]

These banks also approach operational risk, and cyber within it, similarly within their corporate management and governance frameworks. With slight variation in nomenclature and organization, the large banks studied here follow this same general approach to operational risk oversight. Management is responsible for the design and implementation of an effective operational risk management schema, and for its day-to-day oversight. These operational risk frameworks and programs are situated within the bank's broader system of enterprise risk management.[27] Such operational risk management frameworks share several central tenets: identifying operational risk; assessing and/or measuring found risks; and escalating and reporting known risks when appropriate.[28] As a good example of the language that banks use to explain to their shareholders and investors how the system works, JP Morgan describes in its 2017 Annual Report:

> *The Firmwide Control Committee ("FCC")* provides a forum for senior management to review and discuss firmwide operational risks, including existing and emerging issues and operational risk metrics, and to review operational risk management execution in the context of the Operational Risk Management Framework ("ORMF"). The

25. WELLS FARGO 2017 ANNUAL REPORT, *supra* note 19, at 67.

26. *Compare* Citigroup Inc., Annual Report (Form 10-K) 117 (Feb. 23, 2018), *with* Citigroup Inc., Annual Report (Form 10-K) 106 (Feb. 22, 2019) (directing the reader's attention to the addition of cyber risk language in Form 10-K filings).

27. For an authoritative text on enterprise risk management, see generally GEOFFREY MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE (2015). Enterprise risk management, a term ubiquitous in the corporate governance literature, refers to "a process, effected by an entity's board of directors, management, and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objective." *Enterprise Risk Management*, U. CAL: OFF. PRESIDENT, https://www.ucop.edu/enterprise-risk-management/procedures/what-is-erm.html [https://web.archive.org/web/20190323174741/www.ucop.edu/enterprise-risk-management/procedures/what-is-erm.html].

28. JP MORGAN 2017 ANNUAL REPORT, *supra* note 17, at 79; WELLS FARGO 2017 ANNUAL REPORT, *supra* note 19, at 66–67; Wells Fargo, Form 10-Q, Q3 2018, *supra* note 17, at 29; *see, e.g.*, Bank of Am. Co., Form 8-K, *supra* note 17, at 79 ("A sound internal governance structure enhances the effectiveness of the Corporation's Operational Risk Management Program and is accomplished at the enterprise level through formal oversight by the Board, the ERC, the CRO and a variety of management committees and risk oversight groups aligned to the Corporation's overall risk governance framework and practices.").

> ORMF provides the framework for the governance, risk identification and assessment, measurement, monitoring and reporting of operational risk. The FCC is co-chaired by the Chief Control Officer and the Firmwide Risk Executive for Operational Risk Governance. The FCC relies on the prompt escalation of operational risk and control issues from businesses and functions as the primary owners of the operational risk. Operational risk and control issues may be escalated by business or function control committees to the FCC, which in turn, may escalate to the FRC, as appropriate.[29]

The banks' Boards of Directors are also crucially involved.[30] As earlier noted, bank boards' roles in risk management have increased over the past ten years as an area of increasing regulatory and shareholder concern.[31]

As part of this trend, boards are expected to have oversight of cyber risks, too, as cyber incidents expose the firm to reputational and legal risk. Accordingly, boards are generally expected to hold managers accountable for the creation and maintenance of effective risk management programs, ensuring that information technology is up to date.[32] In a nutshell, the board has primary oversight responsibility for the operational risk management framework.[33] Synthetizing management and board responsibilities, these banks characterize their operational risk management strategy as employing "three lines of defense": the first line including responsibilities for risk monitoring imposed on business units; the second line involving compliance personnel; and the third line, internal audit.[34] That said, it is not clear if and

---

29. JP MORGAN 2017 ANNUAL REPORT, *supra* note 17, at 79.

30. It bears noting, however, it would be highly unlikely for the board to be held legally liable for a lapse in the bank's cyber defenses under Delaware and analogous state corporate law principles. *See generally* Stone *ex rel* AmSouth Bancorporation v. Ritter, 911 A.2d 362 (Del. 2006) (limiting liability to cases where directors and officers "utterly failed to implement any reporting or information systems or controls"); *In re* Goldman Sachs Group, Inc. S'holder Litig., No. 5215-VCG, 2011 WL 4826104 (Del. Ch. Oct. 12, 2011) (rejecting liability for risk taking in the absence of red-flags); *In re* Citigroup Inc. S'holder Derivative. Litig., 964 A.2d 106 (Del. Ch. 2009) (suggesting there is limited legal liability for a board's failure to monitor for risk).

31. *See* Martin Lipton, *Risk Management and the Board of Directors*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Feb. 15, 2017), https://corpgov.law.harvard.edu/2017/02/15/risk-management-and-the-board-of-directors-4 [https://perma.cc/L9C2-E2ES].

32. *See* Christopher P. Skroupa, *Cybersecurity and the Board's Responsibilities—'What's Reasonable Has Changed,'* SKYTOP STRATEGIES (Apr. 19, 2018), https://skytopstrategies.com/cybersecurity-boards-responsibilities-whats-reasonable-changed [https://perma.cc/D9ET-7KBF] (interviewing Michale Yeager, a thought leader in the cybersecurity law industry).

33. *See, e.g.*, Wells Fargo, Form 10-Q, Q3 2018, *supra* note 17, at 28–29.

34. *See, e.g.*, Citigroup Inc., Annual Report, *supra* note 26, at 60; *see also* EY, A SET OF BLUEPRINTS FOR SUCCESS 9 (2016), *available at* https://www.ey.com/Publication/vwLUAssets/ey-a-working-set-of-blueprints-to-deliver-sustainable-returns/$FILE/ey-a-working-set-of-blueprints-to-deliver-sustainable-returns.pdf [https://perma.cc/C3WQ-8XN4] (providing a chapter titled "Implementing the Blueprint for Managing Risk More Effectively").

how these banks will adapt the three-lines model to the specific context of cyber risk.

B. DISCLOSURE AND OPERATIONAL RISK

As with other forms of business risk, the securities law requires public companies to disclose certain information about operational risk and the management of this kind of risk. As one form of regulatory tool, disclosure can indeed shape behavior. In the cyber context, by providing the market with information about a bank's cyber risk (and its systems for controlling cyber risk), disclosures equip shareholders with the information they need to hold bank managers accountable for properly managing the risk and enable the market to discipline banks that do poorly at that job.[35]

Banks, like all public companies, are required to keep the public apprised of their operational risk management in a variety of ways.[36] Perhaps the most important vehicles for the delivery of such information are the periodic filings that banks must provide via SEC Form 10-Q and SEC Form 10-K; reports of "material" events that affect the banks on SEC Form 8-K; and the proxy statements that are provided to shareholders before their annual meetings. These forms require the disclosure of cyber 'issues,' broadly speaking, in a variety of different circumstances and on a range of different triggers.

For one, a bank might be required to disclose a cyber attack, breach, etc., on SEC Form 8-K if it is considered "material." These filings are known as "current report[s]," and should be used by companies "to announce major events that shareholders should know about."[37] Companies have four business days to file a Form 8-K after a specified trigger.[38]

However, the critical question is whether any given cyber event falls within the definition of "material." The SEC has stipulated several kinds of events that should trigger the requirement to file an 8-K, that is, which events are "material." Examples include changes in control, material modifications to rights of security holders, amendments to bylaws, and submission of matters to a shareholder vote. Beyond that, as one can imagine, the interpretation of what kind of event is "material" can and does vary widely. The SEC also provides that there are "other events" that could trigger a filing, which are

35. *See infra* Section IV.A (discussing these theories in detail). While the original purported justification for adding mandatory disclosure to the post-depression financial legislation was grounded in investor protection, see Frank H. Easterbrook & Daniel R. Fischel, *Mandatory Disclosure and the Protection of Investors*, 70 VA. L. REV. 669, 670 (1984), as will be seen, that justification has been eclipsed by economic rationales since the early 1980s.

36. Mandatory disclosure requirements generally fall into two categories—one, which apply to an initial or subsequent public offering and sale of a company's securities; and another, which apply periodically. Here, I focus on the latter as the ideal indicator of how banks are informing the public about ongoing and evolving cyber risks.

37. *Form 8-K*, SEC, https://www.sec.gov/fast-answers/answersform8khtm.html [https://perma.cc/X22V-4VZ5]. This requirement is imposed by the Securities Exchange Act of 1934.

38. *Id.*

explained as "events that are not specifically called for by Form 8-K, that the registrant considers to be of importance to security holders."[39] A cyber intrusion or cyber breach could arguably fall under the "other events" category. In that domain, however, disclosure remains optional.

Banks are also required to file periodic reports, which require some disclosure of various risks and information about internal controls. Here, too, one could interpret some requirement to disclose cyber issues. Forms 10-Q and 10-K are the two main forms that public companies must file on an ongoing basis. The 10-Q is filed quarterly, for the first three quarters of each fiscal year and "includes unaudited financial statements and provides a continuing view of the company's financial position during the year."[40] Companies are not, however, specifically required to discuss operational risks in the Form 10-Q.[41]

The annual report on Form 10-K goes further in reaching cyber risks. 10-Ks must be filed annually and include an overview of the company's business, its financial condition, and audited financial statements.[42] (It bears noting that the annual report on the 10-K is different from the glossy "Annual Report to Shareholders" that companies tend to send to their shareholders before meetings.)[43] There are two sections in particular where one could expect to find disclosure relating to cyber security or cyber incidents. For one, the SEC requires the registrant company to disclose "the most significant factors that make investments in the company's securities speculative or risky" under Item 1A of the Form 10-K.[44] The SEC expects quantitative as well as qualitative risks to be reported therein.[45] Item 503(c) requires separate explanation of each risk factor.[46] In recent months, lawyers have advised firms to consider whether cyber fits into the risk factor milieu.[47]

---

39. *Id.*

40. *Form 10-Q*, SEC, https://www.sec.gov/fast-answers/answersform10qhtm.html [https://perma.cc/BJK9-R8VT].

41. Wells Fargo probably only did so given its unique regulatory circumstances—it had entered into a consent order with the Federal Reserve regarding identified weaknesses in its governance and compliance and risk management structures. *See Wells Fargo Update: Federal Reserve Consent Order*, WELLS FARGO, https://www08.wellsfargomedia.com/assets/pdf/about/investor-relations/presentations/2018/consent-order-prepared-comments.pdf [https://perma.cc/B88N-5EEU].

42. *Form 10-K*, SEC, https://www.sec.gov/fast-answers/answers-form10khtm.html [https://perma.cc/BJK9-R8VT].

43. *Id.*

44. *SEC Cyber Guidance*, *supra* note 4, at 10; *see also* 17 C.F.R. § 229.503(c) (2017).

45. *See* 17 C.F.R. § 229.305.

46. EY, SEC FINANCIAL REPORTING SERIES: 2017 SEC ANNUAL REPORTS—10-K, at 43 (2017), *available at* https://www.ey.com/Publication/vwLUAssets/SECAnnualReports10K_06546-171US_21November2017/$FILE/SECAnnualReports10K_06546-171US_21November2017.pdf [https://perma.cc/C45E-597D].

47. *See, e.g.*, *Key Considerations for Fiscal Year 2018 Form 10-K and 20-F Filings*, SULLIVAN & CROMWELL LLP (Dec. 19, 2018), https://www.sullcrom.com/files/upload/SC-Publication-Key-

Additionally, one might expect to see discussion of operational risks, including, now, cyber risks, in the Management Discussion & Analysis ("MD&A") section of the Form 10-K. The MD&A is a "narrative explanation" of the company's financial picture, intended to "enhance a readers' understanding of its financial condition, changes in financial condition and results of operation."[48] Presumably, the MD&A is a prime location to discuss qualitative risks to the business, alongside some backward and forward-looking assessment of the risk, and the governance and controls in place to mitigate (and, when needed, react to) the risk.

Finally, there are also SEC rules surrounding information that must be included with a company's proxy materials that could extend to cyber issues.[49] Along with the proxy statement, companies must provide an annual report that includes (at least) the audited financial statements and the other information required by Rule 14a-3 of the Exchange Act. The requirements for this annual report are not the same as those imposed on the Form 10-K; some companies choose to deliver the glossy, more appealing annual report to shareholders while others simply provide the annual report that accompanies Form 10-K.[50] The proxy annual report must have an MD&A of financial condition and results of operation, as well as quantitative and qualitative disclosures about market risk.[51]

Importantly, in 2009, the SEC adopted more specific standards for the disclosure of risks on the proxy statement. Now, companies must disclose how the board oversees risk management, whether this is organized as a committee or the responsibility of the board as whole, and how the board acts to monitor risk.[52] As the SEC noted at the time it adopted that enhanced disclosure requirement, "We were persuaded by commenters who noted that risk oversight is a key competence of the board, and that additional disclosures would improve investor and shareholder understanding of the role of the

Considerations-for-Fiscal-Year-2018-Form-10-K-and-20-F-Filings.pdf [https://perma.cc/N5MW-GJKH].

48. SEC, FINANCIAL REPORTING MANUAL: TOPIC 9—MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL POSITION AND RESULTS OF OPERATIONS 9110.1, *available at* https://www.sec.gov/corpfin/cf-manual/topic-9 [https://perma.cc/4FKY-H2WB].

49. The Securities Exchange Act of 1934 requires registered companies to file a proxy statement prior to a shareholder meeting.

50. 17 C.F.R. § 240.14c-3 (2018); Annual Report (Form 10-K), Fed. Sec. L. Rep. (CCH) ¶31,101, at 22,063 (allowing the 10-K to incorporate the annual report by reference).

51. These are items 303 and 305 of Regulation S-K, respectively. *See* EY, SEC FINANCIAL REPORTING SERIES: 2018 PROXY STATEMENTS 18 (2017), *available at* https://www.ey.com/publication/vwluassetsdld/2018proxystatements_06548-171us_30november2017/$file/2018proxystatements_06548-171us_30november2017.pdf?OpenElement [https://perma.cc/ECF2-GTG9].

52. Proxy Disclosure Enhancements, Release Nos. 33-9089; 34-61175, 74 Fed. Reg. 68,334, 68,337 (Dec. 23, 2009). These rules amended Rule 407 of Regulation S-K.

board in the organization's risk management practices."[53] The SEC noted that the rule refers to a "variety of risks," including "operational risk."[54]

While the face of the rules surrounding these filings may be subject to interpretation when it comes to cyber issues, the SEC has attempted to clarify its expectations surrounding cyber disclosures through interpretive guidance. First, in October 2011, the SEC's Division of Corporate Finance issued a guidance document regarding registered companies disclosure obligations relating to cybersecurity risks and incidents.[55] Noting the "more frequent and severe cyber incidents" in the years preceding, the Guidance explained: "Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents."[56]

The guidance then specifically called out the Risk Factor section, Item 1A, on the Form 10-K, and the MD&A section, Item 7 on the Form 10-K, as specific obligations that might warrant a cyber disclosure.[57] As for the Item 1A Risk Factors, the Guidance explained:

> [W]e expect registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption.[58]

Indeed, the guidance appeared to require a significant degree of specificity in a given risk disclosure. As an example, it gave the possibility of a cyber attack involving malware that is embedded in systems and results in the compromise of customer data. The SEC made clear, "it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur."[59] More detail would be expected: "Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and

53. *Id.* at 68,345.

54. *Id.*

55. *CF Disclosure Guidance: Topic 2*, SEC (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [https://perma.cc/6BR6-E6VJ].

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.*

potential costs and consequences."[60] It did qualify that the SEC would not expect disclosure that would compromise the company's cybersecurity.[61]

On the MD&A, the SEC set a similar standard in the cyber guidance. Registered companies should disclose cyber issues in this section of the Form 10-K "if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition."[62]

The SEC reiterated and expanded this cyber disclosure guidance in February 2018.[63] For the most part, the 2018 guidance re-emphasized the 2011 guidance but with a slightly more urgent tone: "Given the frequency, magnitude and cost of cybersecurity incidents, . . . it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion . . . ."[64] The guidance emphasized the importance of timely disclosure in the periodic reports: Forms 10-K and 10-Q. Expanding on the 2011 guidance, it also noted the importance of the current reports, Form 8-K. It "encourage[d]" filing companies to increase their use of that form to make cybersecurity disclosures, stating that such "practice" would "reduce[] the risk of selective disclosure, as well as the risk that trading in their securities on the basis of material non-public information may occur."[65]

Through these two guidance documents, the SEC appears serious about cyber risk and incident disclosure. In a Press Release accompanying the 2018 Guidance, SEC Chairman Jay Clayton underscored the purpose of the Guidance—to "promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors."[66] But the question remains whether doubling-down on disclosure in this manner is justified. Are disclosures effective in addressing the social interest in cyber risk in banks and, if so, are the current disclosure requirements optimally designed to accomplish the relevant goals?

The rest of the Article takes up that question. Part III considers what banks are disclosing about their cyber issues by examining the contents of banks' SEC filings. Part IV then engages in an economic analysis of how well disclosure, as a regulatory tool, addresses the market failures specific to cyber risk in banks.

---

60. *Id.*
61. *Id.*
62. *Id.*
63. *See SEC Cyber Guidance*, *supra* note 4, at 1.
64. *Id.* at 4.
65. *Id.* at 10.
66. Clayton, *supra* note 4.

III. DATA ON DISCLOSURE

As Part II explained, the largest, systemically important banks agree that managing operational risk is a core part of their business, for which managers and boards are responsible. These banks likewise agree that cyber risk is now a key component of operational risk. Given the prevailing securities law regarding risk disclosure and governance, these facts suggest that banks can and should be required to disclose a wide range of information about their cyber issues. And indeed, as just discussed, the SEC has "guided" public companies that such disclosures are within the ambit of their required filings in their periodic and event reporting, and in their proxy materials. This Part takes a fact-based approach to assessing the design of the SEC's cyber disclosure guidance. To do that, it takes a deep dive into what and how banks are currently disclosing about their exposure to cyber risk.

A. METHODOLOGY

What follows explains my approach to (and rationale for) the data-gathering and analysis. Specifically, it sets out detail on the sample size and selection, the time-horizon chosen, the content searched for in each filing, and the descriptive typology I constructed for classifying each cyber reference I found in the disclosures.

The Sample. As set out above, I focus on banks and, in particular, the largest internationally active banks. I focus on these banks because of their special role in the U.S. and global economies, as a result of their size and interconnectedness. As the Article urges, in light of their special social and economic role, an optimally designed disclosure regime for these banks depends on understanding the relationship between the disclosure of their cyber information and the interaction of several relevant regulatory goals: price efficiency, accountability to shareholders through appropriate corporate governance structures, and financial stability.

Accordingly, my data draws from the SEC filings of the seven largest internationally active banks, by total assets and exposures, which have also been designated as global systemically important financial institutions ("G-SIBs"): JP Morgan Chase, Citigroup, Bank of America, Wells Fargo, Goldman Sachs, BNY Mellon, and Goldman Sachs.[67] For further legal context, the Dodd-Frank Act of 2010 sets a $50 billion-dollar threshold, and institutions with assets equal to or above that threshold are regulated according to the Federal Reserve's framework for systemically important banks. Those regulations include, among others, heightened capital standards,[68] which

67. *See* OFFICE FIN. RESEARCH, G-SIB UPDATES 1 (2017), *available at* https://www.financialresearch.gov/gsib-scores-chart/files/GSIB_Figures_Dec21.pdf [https://perma.cc/X8YU-JR3A]. For reference, "G-SIB" stands for global systemically important bank.

68. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 165, 124 Stat. 1376, 1423 (2010). Section 171 of the Act required the leverage and risk-based capital

stem from the Fed's implementation of the internationally agreed Basel III Accords.[69] They also include requirements for capital planning and stress testing, the preparation of resolution plans (sometimes known as 'living wills') and various programs of risk management.[70]

The Content Searched. I then hand-collected these banks' SEC filings on Form 10-K, Form 8-K, and their proxy materials. Why focus on this set of forms? For one, the SEC has explicitly called out the importance of these three forms in various pieces of interpretative guidance specific to operational risk over the past 15 years.[71] So it seemed legally reasonable to expect that the locus of cyber disclosure would be consolidated across these materials. Moreover, because these three forms are among the most publicly visible among the universe of SEC forms, it also seemed reasonable to presume that firms would use them to disclose their cyber issues—or at least it seemed fair to assume that they should be doing so.

Again, to recap what was earlier discussed, the Form 10-K is an opportunity to "tailor risk factors generally, and the occurrence of a[] . . . cybersecurity event provides fodder for such fine tuning."[72] The Form 8-K meanwhile, is intended to update shareholders about events that a reasonable shareholder would find significant: changes in internal governance, regulatory proceedings, or the undertaking of a financial obligation are all events that trigger an 8-K filing. An uptick in cyber risk, or an actual cyber event, could also fall under the 8-K purview. Lastly, if a cyber issue impacts the board's oversight of risk generally, that information should be contained in the proxy statement.[73]

Time Horizon. I collected this assortment of filings over a three-year period, starting January 1, 2016, and ending December 31, 2018. I limited the data to a three-year span given the pace at which cyber risks have materialized. Prior to 2016, banks' attention was far less focused on operational risk issues, as they were still reeling from the regulatory impact of

---

requirements that apply to depository institutions to apply to all "bank holding company[ies]." *Id.* § 171. This section of the Dodd-Frank Act became known as the "Collins Amendment."

69. BASEL COMM. ON BANKING SUPERVISION, BASEL III: A GLOBAL REGULATORY FRAMEWORK FOR MORE RESILIENT BANKS AND BANKING SYSTEMS 54–57 (2011), https://www.bis.org/publ/bcbs189.pdf [https://perma.cc/3R9P-YMJT].

70. *See generally* MARC LABONTE & DAVID W. PERKINS, CONG. RESEARCH SERV., R45036, BANK SYSTEMIC RISK REGULATION: THE $50 BILLION THRESHOLD IN THE DODD-FRANK ACT (2017), *available at* https://fas.org/sgp/crs/misc/R45036.pdf [https://perma.cc/ZPA4-SB79] (reviewing the various requirements of the Dodd-Frank Act across risk and risk management areas). For further detail on this regime, see *infra* Section III.B.

71. *See supra* Section II.B.

72. Luke Dembosky & Jeremy Feigelson, *How to Disclose a Cybersecurity Event: Recent Fortune 100 Experience*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Sept. 26, 2016), https://corpgov.law.harvard.edu/2016/09/26/how-to-disclose-a-cybersecurity-event-recent-fortune-100-experience [https://perma.cc/MHA8-7XQ5].

73. While there are other key forms mentioned in the SEC guidance, many are for foreign issuers, so they are not considered here.

the financial crisis and much more concerned with balance sheet strengthening. The same could be said of regulatory priority. I thus hypothesized that disclosures of cyber issues would be scant in earlier years. Moreover, I hypothesized that the fall 2017 Equifax breach and winter 2018 SEC guidance would be highly influential in bank behavior—and so I presumed that reviewing the banks' filings in the year before Equifax and comparing them with filings the year after Equifax, and the year after the SEC Guidance, would yield fruitful results.

This collection of filings, over this time horizon, yielded a data set of 895 SEC filings.

Cyber References. I then reviewed each of these filings in search of cyber references. My general approach was to gather information from the filings along quantitative and qualitative dimensions.

On the quantitative side, I wanted to present a picture of how *much* these banks are publicly discussing their cyber issues. To that end, I reviewed each of the 895 filings for any cyber 'reference.' I made some subjective judgments about how to count such references: I counted as one reference any consolidated discussion of a cyber issue. So, for example, if there was one isolated reference to a "cyber-risk oversight committee" or a non-interest expense owing to "cyber controls," each such reference would be counted once. If, however, there was an extended discussion of cyber risk as an operational risk, which spanned three pages, so long as the discussion was presented under one umbrella heading—i.e., operational risk management—that was also counted as one reference. Ultimately, I determined that grouping references in this way would give the most accurate sense of how frequently firms are discussing cyber on any given score, without inflating the findings.

I also excluded some kinds of references. In particular, I excluded references to any factual statement about the governing legal regime, because I assumed that this kind of discussion would not involve the bank disclosing a cyber issue unique to that bank.[74] I also excluded references to cyber if those references were connected to a statement about a director's background or experience, or about director criteria. There were many such biographical references. In my view, such references would not provide a sense of risk or incident, or a specific method of procedure or control.[75] Lastly, I excluded

74. *E.g.*, JP Morgan Chase & Co., Annual Report (Form 10-K) 7 (Feb. 27, 2018) ("The Firm and its subsidiaries are subject to federal, state and international laws and regulations concerning the use and protection of certain customer, employee and other personal and confidential information, including those imposed by [list of laws]. In addition, various U.S. regulators . . . have increased their focus on cybersecurity . . . through guidance, examinations and regulations.").

75. There is an argument to be made that capturing this biographical information could have indicated something about the investment in a bank's cyber defense resources, by investing in directors with such experience. Perhaps this will be an area for future study.

references to cyber in connection with banks' caveats for forward-looking statements. Each filing hedges against its forward-looking statements by explaining that those statements may become inaccurate due to a slew of boilerplate events, including some cyber events. Again, such reference has nothing to do with an actual, expected, or perceived cyber issue at the bank.

Reference Typology. I also attempted to present data that captures the nuance among the cyber references. Accordingly, after presenting raw numerical data—tallying the number of cyber references, per bank, per filing-type, per year—I then broke down the references by type. To do so, I developed a descriptive typology which categorizes each reference, by filing, as either an 'organizational/neutral' reference; a 'preventative/investment' reference; or a 'negative/risk disclosure' reference.

The first category, *organizational/neutral*, is meant to capture references that discuss the way in which the bank's management or board deals with cyber as a part of its risk management framework. These tend to speak generally to the bank's enterprise risk management framework. Examples of these types of references are mentions that the board and its committees continue to review their respective oversight responsibilities, including cyber risk. This type of reference is both organizational in nature and relatively neutral. It neither underscores the salience of the cyber risk nor downplays its significance to the bank.

The second category, *preventative/investment*, includes references that speak to the bank's investment in resources that are aimed at addressing cyber risk. Examples of these kinds of references include details about enhancements that a bank has made to its cyber risk management technology. Sometimes, the references are purely financial-oriented, such as a reference to the increase in non-interest expenses owing to an increase in cyber expenses. Unlike the organizational-neutral references, these references tend to be explicitly or implicitly positive—or optimistic—in tone regarding the bank's cyber exposure. The text or subtext of these references is that some form of continued or increased investment will go far in mitigating actual and potential cyber risk at the firm.

The third category of *negative/risk disclosure* references is arguably the most interesting and may well be the most important for purposes of evaluating the actual risk that the bank is facing from a cyber attack. These references disclose actual or potential cyber risks or discuss costs to the bank or financial sector more broadly arising from these risks. This category is also meant to capture bank disclosures of actual cyber incidents; though I did not find any such references. Examples of these types of references generally include statements that the bank is subject to ongoing cyber attacks; statements that these attacks are likely to continue; and various descriptions of the costs that would be associated with a widespread breach. Because of the

importance of this category, it is given a more detailed treatment below, in this Part's qualitative analysis of the data.[76]

Some references naturally shared dual qualities, for example, relating principally to the resources invested in the bank's cyber infrastructure, but also referencing the hierarchy of the bank's cyber risk management. In these cases, I made a judgment call about which purpose in the reference dominated, taking in view the surrounding context (i.e., headings, topic, etc.). I decided to label these kinds of references with only one type-category, in order to present the most accurate picture of the relative proportions of the three kinds of references.[77] Also on the qualitative front, I provided some narrative examples of each type of disclosure. Naturally, the selection is a subset, which I considered representative. I provided the most narrative in connection with the banks' 10-K filings, as the material in those disclosures had the most relevant implications for financial stability regulation.[78]

Overall, I found that the typology added significant color to the numerical distribution. Consider, after all, the difference between a reference to the fact that a bank's cyber committee sits under audit, and a reference to a cyber breach that resulted in the loss of the bank's customer data (hypothetical). In short, as important as it is to know how much firms disclose about cyber, it is equally if not more important to understand *what* they are saying about it.

B. THE FILINGS

Below is a narrative explanation of the key aspects of my findings, on both quantitative and qualitative dimensions.

1. Quantitative Analysis

Across the 895 filings I analyzed, there were 140 cyber references in total. The following discusses the distribution and relative frequency of these disclosures.

By far, the greatest number of filings were the Forms 8-K. This is not surprising given the wide range of triggering events that require a bank to file a Form 8-K. In total, there were 836 Form 8-Ks filed by these seven banks, during 2016, 2017, and 2018. What is surprising, however, is the number of cyber references in these 895 filings: There were 28.

JP Morgan made 13 cyber references across three different 8-K filings. However, on examination, each of these references appears in exhibits featuring investor presentations; none of the references therein discloses a cyber incident. Rather, they discuss cyber risk initiatives and investments. Bank of America made two references in 2016, and Wells Fargo made three

76. *See infra* Section III.B.2.

77. *See infra* Table 1 by type.

78. That connection is explored *infra* Part IV.

in 2017 and seven in 2018. Like the JP Morgan disclosures, all of these banks' 8-K cyber references also fell into the organizational/neutral category, or the preventative/investment category. Neither Citigroup, Goldman Sachs, BNY Mellon, or Morgan Stanley had an 8-K filings with a cyber reference during these three years. In summary, there have been no disclosures of a cyber event—such as a breach, intrusion, or elevated threat level—from these seven banks over a three-year period.

Turning to the proxy statements and materials, all together, there were 38 materials. Though there is usually only one shareholder meeting each year, some of the banks issued a proxy statement as well as some preliminary or related materials before or after the meeting. Here, cyber references were slightly more frequent. Among the seven banks, there were 30 cyber references in the filed forms. Again, however, as with the Form 8-K, none of these references fell into the negative/risk disclosure camp. Twenty-eight of the references were organizational/neutral, and 13 were preventative/investment.

The picture with the Form 10-Ks was very different. Again, each bank files one 10-K per year. That made for a total of 21 filings that I reviewed. And all of the Form 10-Ks had at least one—but as many as five—meaty sections of cyber discussion. I counted each section as one reference, for the reasons discussed above. All of the 10-Ks discussed cyber in Item 1A, regarding "Risk Factors," and 11 of the 10-Ks also discuss cyber in the MD&A. Interestingly, the lion's share of these references are in the negative/risk disclosure category—45 of the 71 total references. The balance of the references consisted of 12 preventive/investment references, and 14 organizational/neutral references.

The following tables summarize these results.

Table 1. The Number of Cyber References by Filing Type

	8-K	Proxy	10-K
JP Morgan Chase	112 filings	9 filings	3 filings
2016	7	5	4
2017	4	2	3
2018	2	4	4
Bank of America	75 filings	14 filings	3 filings
2016	2	0	2
2017	0	0	1
2018	0	4	2
Citigroup	99 filings	3 filings	3 filings
2016	0	1	1
2017	0	1	1
2018	0	2	2
Wells Fargo	412 filings	3 filings	3 filings
2016	0	4	3
2017	3	2	3
2018	7	6	4
Goldman Sachs	47 filings	3 filings	3 filings
2016	0	1	3
2017	0	1	4
2018	0	0	5
BNY Mellon	55 filings	3 filings	3 filings
2016	0	0	4
2017	0	0	3
2018	3	1	4
Morgan Stanley	36 filings	3 filings	3 filings
2016	0	1	5
2017	0	3	6
2018	0	3	7

Table 2. A Typology of Cyber References

	8-K	Proxy	10-K
Organizational/Neutral	6	28	14
Preventive/Investment-related	22	13	12
Negative/Risk Disclosure	0	0	45

2. Qualitative Analysis

This data reveals somewhat of a mixed picture of bank disclosures of their exposure to cyber issues.

Above, Table 2 sets out the frequency of references according to their type. It shows that organizational-neutral references were most common, with 48 of the 140 total references falling in this category. Most of these references were in the proxy statements or accompanying proxy materials. For example, JP Morgan's April 5, 2018 proxy statement included a letter from Jamie Dimon, the chairman, and Lee Raymond, lead independent director, to the shareholders, in which they explained that "[c]yber defense and improving our resiliency against cybersecurity threats remains a key focus at all levels of management within the Firm, and of your Board."[79] While that kind of reference is more organizational, insofar as it demonstrates that cybersecurity is within the purview of corporate governance, other references in this category are more factual. For instance, in Bank of America's March 12, 2018 proxy statement, the bank stated that cyber risk is one of the seven kinds of risk that the bank faces and the board oversees.[80] This kind of statement is both organizational and neutral by conveying that cyber risk is a board issue, thus the reference is situated squarely in this category.

I also included as organizational/neutral any references to cyber in the context of justifying an executive's compensation. This categorization made sense, as the reference was organizational insofar as it discussed the executive's performance of his duties, and relatively neutral insofar as an assessment of the actual risk was concerned. For instance, in Citigroup's 2016 Proxy Statement, it mentions in its compensation discussion and analysis, that the head of operations and technology leads efforts in the cybersecurity arena and initiates new approaches to developing cybersecurity talent.[81] On the whole, this type of reference mainly states that cyber is a risk to the firm and explains, in varying detail, how management and the board address it. As a final example, Wells Fargo added a new section to its 2018 Proxy Statement specific to the board's oversight of cyber risk:

> [O]ur Board is actively engaged in the oversight of our Company's information security risk management and cyber defense programs. The Risk Committee receives regular updates and reporting from the Company's Chief Information Security Officer, head of the

79. JPMORGAN CHASE & CO., ANNUAL MEETING OF SHAREHOLDERS PROXY STATEMENT 5 (Apr. 5, 2018), *available at* https://www.jpmorganchase.com/corporate/investor-relations/document/proxy-statement2018.pdf [https://perma.cc/3LXC-AB8G] [hereinafter JP MORGAN, 2018 PROXY STATEMENT].

80. Bank of Am. Co., Proxy Statement (Schedule 14A) 28 (Mar. 12, 2018) [hereinafter Bank of America, 2018 Proxy Statement].

81. CITIGROUP, 2016 PROXY STATEMENT 68 (Mar. 16, 2016), *available at* https://www.citigroup.com/citi/investor/quarterly/2016/ar16cp.pdf?ieNocache=389 [https://perma.cc/J9HH-4D2J].

> Cyber Defense Program, and head of Enterprise Information Technology on our information security/cyber risk strategy, cyber defense initiatives, cyber event preparedness, and cyber security risk assessments.[82]

In summary, what we see from this qualitative sampling of the organizational/neutral disclosures is that these large U.S. banks are dedicating most of their cyber disclosure to (1) informing investors that cyber risk is a part of the firm's governance structure; (2) detailing how the risk management structure has adapted to include cyber issues; and (3) in various other forms, setting out which committees, board members or executives are focused on the issue. The message from banks to shareholders and the SEC: We know that cyber is a risk, and we are well-organized to address it. Thus, while the references may be mostly neutral on their face, the their tone is moderately positive.

Closely behind organizational/neutral is the frequency of preventative/investment references. Of the 140 total cyber references, 47 were in this category. All of these references discuss, in one way or another, how the bank is dedicating or deploying resources to reduce cyber risk. The difference between this category and organizational/neutral is subtle. The distinction is that organizational/neutral references are intended to capture information about how the firm is organized to deal with risk (or instances where the bank acknowledges the risk); whereas the preventive/investment category captures information about the amount or kind of resources the bank is deploying to *prevent* a risk from materializing (or to mitigate costs if it does). While both types of reference seem framed to reassure investors, the preventative/investment resources are slightly more positive and emphatic than the organizational/neutral ones.

For example, in its 2018 Proxy Statement Wells Fargo spoke about its efforts to "transform[] the bank," and its "journey and progress to rebuild trust," along risk management and accountability dimensions; specifically, the bank stated that it had "[i]nvested over 2016 and 2017 in technology risk, including cybersecurity, with additional investments expected in 2018."[83] Other references are more direct in explaining the bank's expenditure: According to JP Morgan's 2016 Proxy Statement, it "increased cybersecurity spending from approximately $250 million in 2014 to approximately $500

82. WELLS FARGO & CO., 2018 ANNUAL MEETING OF SHAREHOLDERS: PROXY STATEMENT 45 (Mar. 14, 2018), *available at* https://wwwo8.wellsfargomedia.com/assets/pdf/about/investor-relations/annual-reports/2018-proxy-statement.pdf [https://perma.cc/XV36-LGXR].

83. *Id.* at 5–7. Now, to be fair, Wells Fargo may well have special reasons for over-emphasizing its dedication to risk management and investing in improvements, as it was the subject of regulatory action for identified weaknesses on those scores.

million in 2015, as there is no investment more important than protecting the data and assets of the Firm, and our customers and clients."[84]

Most of these preventative/investment references are similarly worded. JP Morgan's 2017 Proxy Statement disclosed that the "Firm devotes significant resources . . . . [and] continue[s] to make significant investments in enhancing our cyber defense capabilities[,] . . . to understand the full spectrum of cybersecurity risks in the environment, [and] to enhance defenses and improve resiliency against cybersecurity threats."[85] Within the same reference, the bank went on to state that "[g]lobally, thousands of employees are focused on cybersecurity."[86]

Another common preventative/investment disclosure dealt with non-interest expenses—usually those expenses increase due to a range of regulatory, professional services, and technology expenses; cyber is included.[87] Bank of America had one slightly unique preventative/investment reference, whereby it disclosed that it arranges for its directors to hear from regulators on cybersecurity topics.[88] Again, a similar gist to the organizational/neutral references—insofar as the messaging is generally positive—with slightly more granular details in this category about how the bank is seeking to minimize the impact of its cyber exposure.

The third category includes negative/risk disclosure references. Now, to be clear, I did not find any bank disclosure of cyber events—that is to say that no bank used a Form 10-K (or Form 8-K) to disclose an actual cyber incident or breach. However they did use 10-K filings to discuss potential or imminent cyber risks. These types of references are qualitatively different from the others, as they speak to actual cyber risk or incident (in a general fashion), potential cyber risk or incident, and the costs to the firm or financial system more broadly: their cyber "exposure," so to speak.

I found all of these references in the annual reports of the Form 10-K.[89] It is also interesting to note that there is no meaningful change in the distribution of these types of references between 2016, 2017 or 2018, despite the SEC's issuance of the 2018 cyber guidance (which would have impacted

84. JPMORGAN CHASE & CO., ANNUAL MEETING OF SHAREHOLDERS PROXY STATEMENT 41 (Apr. 7, 2016), *available at* https://www.jpmorganchase.com/corporate/investor-relations/document/proxy-statement2016.pdf [https://perma.cc/8QB2-33EU].

85. JPMorgan Chase & Co., Proxy Statement (Schedule 14A) 38 (Apr. 5, 2017).

86. *Id.*

87. *See, e.g.*, Press Release, Wells Fargo, Wells Fargo Reports Third Quarter 2017 Net Income of $4.6 Billion; Diluted EPS of $0.84 Included the Impact of a Discrete Litigation Accrual of $(0.20) Per Share for Previously Disclosed Mortgage-related Regulatory Investigations (Oct. 13, 2017), *available at* https://www08.wellsfargomedia.com/assets/pdf/about/investor-relations/earnings/third-quarter-2017-earnings.pdf [https://perma.cc/VH8R-S958] (a news release in connection with its third quarter 2017 results).

88. Bank of America, 2018 Proxy Statement, *supra* note 80, at 73–74.

89. In the case of Wells Fargo, one of these references came from its 10-Q filed for the third quarter of 2018. *See* Wells Fargo, Quarterly Report (Form 10-Q) 29–30 (Oct. 24, 2018).

the 2018 10-K reports)—each of the banks consistently dedicated between one and five sections to some discussion of cyber.

These negative/risk disclosure references can be broken down further. There are those that are disclosing the fact that banks are subject to cyber attacks or incidents generally; those disclosing potential or imminent incidents; and those disclosing the projected costs of these incidents. All seven of the banks made such disclosures in their Form 10-Ks, and in some cases the 10-K disclosures increased slightly in detail or urgency over the three-year period studied.[90]

First, consider the references disclosing actual risk. JP Morgan was relatively taciturn about cyber risks in its 2016 10-K. Nonetheless the disclosure was there:

> JPMorgan Chase and other companies . . . have reported significant breaches in the security of their websites, networks or other systems, some of which have involved sophisticated and targeted attacks intended to obtain unauthorized access to confidential information, destroy data, disrupt or degrade service, sabotage systems or cause other damage, including through . . . cyber attacks . . . .[91]

In 2017, its message was exactly the same: "JPMorgan Chase experiences numerous cyberattacks on its computer systems, software, networks and other technology assets on a daily basis."[92] Again, the 2018 filing reiterated the same message: "JPMorgan Chase experiences numerous cyberattacks on its computer systems, software, networks and other technology assets on a daily basis."[93] It added, "JPMorgan Chase has experienced security breaches due to cyberattacks in the past, and it is inevitable that additional breaches will occur in the future. Any such breach could result in serious and harmful consequences for JPMorgan Chase or its clients and customers."[94]

Bank of America was also explicit about the nature of past cyber intrusions (generally) and future cyber risk exposure in its 2016 10-K.

> We, our customers, regulators and other third parties have been subject to, and are likely to continue to be the target of, cyberattacks. These cyberattacks include computer viruses, malicious or destructive code, phishing attacks, denial of service or information or other security breaches that could result in the unauthorized release, gathering, monitoring, misuse, loss or destruction of confidential, proprietary and other information of ours, our

90. *See infra* notes 91–93 and accompanying text.

91. JPMorgan Chase & Co, Annual Report (Form 10-K) 17 (Feb. 28, 2017). This reference appeared in Item 1A of the Form 10-K.

92. JPMorgan Chase & Co., Annual Report (Form 10-K) 18 (Feb. 27, 2018) [hereinafter JP Morgan, 2017 Form 10-K]. This reference also appeared in Item 1A of the Form 10-K.

93. JPMorgan Chase & Co., Annual Report (Form 10-K) 19 (Feb. 26, 2019).

94. *Id.*

> employees, our customers or of third parties, or otherwise materially disrupt our or our customers' or other third parties' network access or business operations.[95]

The same language was repeated, almost word-for-word, in Bank of America's 2017 and 2018 10-Ks.[96]

Citigroup also disclosed in 2016 and 2017 that it has been the subject of multiple, ongoing cyber incidents. Specifically, it reported that "Citi's computer systems, software and networks are subject to ongoing cyber incidents such as unauthorized access, loss or destruction of data (including confidential client information), account takeovers, unavailability of service, computer viruses or other malicious code, cyber attacks and other similar events."[97] The 2017 and 2018 10-Ks used the same language.[98] The 2018 Form 10-K made clear: "Citi has been subject to intentional cyber incidents from external sources over the last several years."[99] The 2018 10-K also dedicated a new section in the MD&A to cybersecurity risk, within the operational risk section.[100]

Wells Fargo took a similar approach. Its 2016 annual report to shareholders (which it incorporated by reference in the Form 10-K) noted: "Wells Fargo and other financial institutions continue to be the target of various evolving and adaptive cyber attacks."[101] Again, an identically worded disclosure was made in the 2017 report, and in the 10-Q filed for the third quarter of 2018.[102] A letter from the Chair of the Board prefacing the 2018

95. Bank of Am. Co., Annual Report (Form 10-K) 11 (Feb. 23, 2017) [hereinafter Bank of America, 2016 Form 10-K].

96. Bank of Am. Co., Annual Report (Form 10-K) 10–11 (Feb. 22, 2018) [hereinafter Bank of America, 2017 Form 10-K]; Bank of Am. Co., Annual Report (Form 10-K) 11 (Feb. 22, 2019) [hereinafter Bank of America, 2018 Form 10-K] (adding "ransomware" as a type of destructive code).

97. Citigroup Inc., Annual Report (Form 10-K) 59 (Feb. 24, 2017) [hereinafter Citigroup, 2016 Form 10-K].

98. Citigroup Inc., Annual Report (Form 10-K) 61 (Feb. 23, 2018) [hereinafter Citigroup, 2017 Form 10-K]; Citigroup Inc., Annual Report (Form 10-K) 54 (Feb. 22, 2019) [hereinafter Citigroup, 2018 Form 10-K].

99. Citigroup, 2018 Form 10-K, *supra* note 98, at 53.

100. *Id.* at 106–07.

101. WELLS FARGO, OUR COMMITMENT: WELLS FARGO & COMPANY ANNUAL REPORT 2016, at 66 (2017), *available at* https://www.wellsfargo.com/assets/pdf/about/investor-relations/annual-reports/2016-annual-report.pdf [https://perma.cc/JY29-8Y3W] [hereinafter Wells Fargo, 2016 Annual Report]; *see also* Citigroup, 2018 Form 10-K, *supra* note 98, at 54.

102. WELLS FARGO, REBUILDING TRUST: WELLS FARGO & COMPANY 2017 ANNUAL REPORT 67 (2017), *available at* https://www.wellsfargo.com/assets/pdf/about/investor-relations/annual-reports/2017-annual-report.pdf [https://perma.cc/7QNG-DB27] [hereinafter Wells Fargo, 2017 Annual Report]; Wells Fargo, Form 10-Q, Q3 2018, *supra* note 17, at 29–30.

annual report to shareholders (which was not incorporated by reference into the SEC form 10-K) noted that "cyber risk is at an all-time high."[103]

Goldman Sachs, in its 2018 10-K report, admitted that it is "regularly the target of attempted cyber attacks, including denial-of-service attacks" and as a result "must continuously monitor and develop [its] systems to protect [its] technology infrastructure and data from misappropriation or corruption."[104] The report goes on to discuss, much as other banks have done, how the evolution and migration to online platforms will increase the bank's exposure to cyber risk in the future; and, despite protective measures, the bank's vulnerability to cyber risk will be impossible to neutralize fully.[105]

Again it bears emphasis that banks were not using the 10-K to disclose the actual cyber incidents that they apparently experienced over the course of a year. Rather, the banks were disclosing the general fact that they were subject to cyber attacks as well as their concerns about future cyber incidents.[106]

Consider a few examples of this kind of language. "A failure in or breach of our operational or security systems or infrastructure, or those of third parties, could disrupt our businesses, and adversely impact our results of operations, liquidity and financial condition, as well as cause [legal or] reputational harm."[107] Such hypotheticals were also included in the Citigroup reports. In 2016, it provided, "[a]s further evidence of the increasing and potentially significant impact of cyber incidents, in recent years, several U.S. retailers and financial institutions and other multinational companies reported cyber incidents that compromised customer data, resulted in theft of funds or theft or destruction of corporate information or other assets."[108] In the 2017 10-K, Citigroup referred to the Equifax breach "[a]s further evidence" to that effect, underscoring that "[t]here can be no assurance that such cyber incidents will not occur again, and they could occur more frequently and on a more significant scale."[109]

The banks have also made statements about possible losses (though all but JP Morgan explicitly claimed that no losses relating to cyber incidents had

103. WELLS FARGO, OUR ROAD AHEAD: WELLS FARGO & COMPANY 2018 ANNUAL REPORT 6 (2019), *available at* https://www08.wellsfargomedia.com/assets/pdf/about/investor-relations/annual-reports/2018-annual-report.pdf [https://perma.cc/5ECA-2VD7].

104. Goldman Sachs & Co, Annual Report (Form 10-K) 31 (Feb. 25, 2019).

105. *See id.* at 31–32.

106. For the legal background on this issue, see, for example, David B. Hennes, *How Safe are the PSLRA Safe-Harbors for Forward Looking Statements*, SEC. LITIG. REP. (July/Aug. 2008), *available at* https://www.friedfrank.com/files/FSTFresource/Articles/Article%2008-08-00%20HowSafe.pdf [https://perma.cc/LY66-UL7M].

107. Bank of America, 2016 Form 10-K, *supra* note 95, at 10.

108. Citigroup, 2016 Form 10-K, *supra* note 97, at 59.

109. Citigroup, 2017 Form 10-K, *supra* note 98, at 61.

yet been "material").[110] One of the lengthier of these loss disclosures is found in Bank of America's 2017 Form 10-K. There, it calls out the range of financial, reputational, and macro risks associated with a cyber attack:

> Cyber attacks or other information or security breaches, whether directed at us or third parties, may result in a material loss or have material consequences. Furthermore, the public perception that a cyber attack on our systems has been successful, whether or not this perception is correct, may damage our reputation with customers and third parties with whom we do business. A successful penetration or circumvention of system security could cause us negative consequences, including loss of customers and business opportunities, disruption to our operations and business, misappropriation or destruction of our confidential information and/or that of our customers, or damage to our customers' and/or third parties' computers or systems, and could result in a violation of applicable privacy laws and other laws, litigation exposure, regulatory fines, penalties or intervention, loss of confidence in our security measures, reputational damage, reimbursement or other compensatory costs, additional compliance costs, and could adversely impact our results of operations, liquidity and financial condition.[111]

Citigroup also mentions the possibility of "financial losses as well as misappropriation, corruption or loss of confidential and other information or assets, which could negatively impact Citi's reputation, customers, clients, businesses or results of operations and financial condition, perhaps significantly."[112] Its 2018 filing goes even further to affirmatively disclose that various cyber incidents had "resulted in limited losses in some instances."[113] Wells Fargo also discloses the possibility that cyber incidents could result in the loss of customers, financial losses, legal losses, or reputational damage.[114] But no details about the actual incidents, timing or otherwise, which caused those losses, is provided.

---

110. *See, e.g.*, Bank of America, 2017 Form 10-K, *supra* note 96, at 11; Bank of America, 2016 Form 10-K, *supra* note 95, at 11 ("Although to date we have not experienced any material losses or other material consequences relating to technology failure, cyber-attacks or other information or security breaches, whether directed at us or third parties, there can be no assurance that we will not suffer such material losses or other consequences in the future."); Citigroup, 2017 Form 10-K, *supra* note 98, at 59–61; Citigroup, 2016 Form 10-K, *supra* note 97, at 59–60; Wells Fargo, 2017 Annual Report, *supra* note 102, at 67; Wells Fargo, 2016 Annual Report, *supra* note 101, at 66.

111. Bank of America, 2017 Form 10-K, *supra* note 96, at 11.

112. Citigroup, 2016 Form 10-K, *supra* note 97, at 59.

113. Citigroup, 2018 Form 10-K, *supra* note 98, at 54.

114. *See* Wells Fargo, 2017 Annual Report, *supra* note 102, at 66–68; Wells Fargo, 2016 Annual Report, *supra* note 101, at 132–34.

As a final example, BNY Mellon's 2018 report discloses that "[a] cybersecurity incident, or a failure to protect our computer systems, networks and information and our clients' information against cybersecurity threats, could . . . adversely impact our ability to conduct our businesses, damage our reputation and cause losses."[115]

The next Part weighs the pros and cons of requiring more detailed information.

* * *

In summary, a documentary analysis of the largest U.S. bank holding companies' cyber disclosures reveals several noteworthy themes and trends:

1. The number of cyber references in these banks' SEC filings is in fact more than one might expect in light of the SEC's guidance, which is premised on the view that public companies are under-disclosing cyber information;
2. Still, the banks were almost uniformly silent in their Form-8Ks about specific cyber risks or incidents;
3. The bulk of cyber references that banks made fell into the organizational/neutral category or the preventative/investment category, which references had a medium to strongly positive tone;
4. Only in Form 10-Ks did banks engage in negative cyber discussion, disclosing risks—real and potential—as well as losses—experienced and possible;
5. The discussion of risk in the 10-Ks was generalized—without reference to specific events—and this discussion was relatively uniform across all seven banks' annual forms.

In light of these themes and trends in the data, the next Part suggests how the SEC might better design its rules (or new guidance) to maximize the private and public interests at stake, and further the relevant regulatory goals.

IV. RE-DESIGNING THE DISCLOSURE RULES

Part III presented a mixed picture of the quantity and quality of bank cyber disclosure. Considering the absolute number of cyber disclosures—in particular 8-K disclosures—one could surmise that banks are under-disclosing their cyber issues. However, on a closer examination of the full range of mandatory disclosures, and in particular the Form 10-Ks, one sees that banks are informing the public about the general nature of their cyber risk exposure and the general direction of the steps they are taking to manage that risk. This

115. Bank of N.Y. Mellon Corp., Annual Report (Form 10-K) 79 (Feb. 27, 2019).

data thus begs the question of optimal regulatory design: Could the SEC better tailor its cyber risk disclosure rules or guidance in light of the interests, incentives, and goals at stake?

Part IV elaborates a framework that the SEC might use to re-assess the design of its current guidance on cyber disclosure. To do that, Part IV first sets out the public and private interests in disclosure and associated regulatory goals. It does so by examining the relevant theoretical justifications for mandatory disclosure in the special context of banks' cyber risk exposure. Part IV then measures banks' existing level of disclosure—as set out in Part III—against these rationales. It then reevaluates what kinds of cyber disclosures might be usefully expanded by rule or guidance, and pinpoints where existing levels of cyber information may already be disclosed in sufficient amounts. Ultimately, this Part urges the SEC's disclosure requirements to be further refined so as to differentiate between event-based disclosure, on the one hand, and procedural and investment-oriented disclosure, on the other.

A. WHERE ARE THE MARKET FAILURES?

As with all financial regulation, mandatory disclosure rules are generally designed to address a market failure.[116] As summarized nicely by Professor John Armour and his co-authors, market failures are regarded as "the failure of markets to achieve the economically efficient outcome with which they are generally associated."[117]

Indeed, there are two classical market failure justifications for mandating public company disclosure—one based on a public goods view of securities research, and another based on information asymmetries between investors and corporate stakeholders. In the case of systemically important banks, there is arguably a third justification based on the view that the operational resilience of each of these banks is also a public good, insofar as each institution's resilience is likely necessary for macro financial stability and, in turn, for real economic activity to thrive.[118]

116. *See* ARMOUR ET AL., *supra* note 15, at 51 ("The design of financial regulation is thus ultimately an exercise in economics—applying the analytic tools of economics to determine the legal and regulatory framework best suited to correcting the failures of a financial system.").

117. *Id.* at 51–52.

118. It bears noting that there are scholars who have put forth non-market failure-based justifications for mandatory disclosure. Those like Professor Paul Mahoney, for example, have argued that the "principal purpose" of mandatory disclosure is to mitigate agency problems, and that "[d]isclosure can help reduce the cost of monitoring [corporate] promoters' and managers' use of corporate assets for self-interested purposes." Paul G. Mahoney, *Mandatory Disclosure as a Solution to Agency Problems*, 62 U. CHI. L. REV. 1047, 1048 (1995); *see also* Zohar Goshen & Richard Squire, *Principal Costs: A New Theory for Corporate Law and Governance*, 117 COLUM. L. REV. 767, 769 (2017).

1. Information about Cyber Risk as a Public Good

The first, perhaps most common rationale advanced in support of mandatory disclosure is grounded in information and has its theoretical roots in the efficient capital markets hypothesis ("ECMH").[119] In broad strokes, ECHM holds that markets price in all available information, and therefore the more information floating around publicly, the more efficient the markets will be. The theory builds on the notion that informational efficiency leads to allocative efficiency.[120] Improvements in allocative efficiency, scholars believe, "impl[y] a more productive economy."[121] But in order to have informational efficiency, markets need information.[122]

But information about corporate securities presents a classic public goods problem.[123] Perhaps the most generative source of information about corporate securities are securities analysts and traders. Traders and analysts are able to get information relatively easily and cheaply, which "increases the aggregate amount of securities research and verification," thereby enhancing informational efficiency.[124] However, because securities analysts cannot exclude others from the research, they cannot obtain the full economic value of their discoveries.[125] This freeriding may result in under-compensation for securities research and, in turn, under-investment in securities research.[126] A mandatory disclosure system can therefore benefit investors by ensuring the

---

119. For a general explanation of efficient capital market hypothesis, see JAMES D. COX, ROBERT W. HILLMAN & DONALD C. LANGEVOORT, SECURITIES REGULATION: CASES AND MATERIALS 91–101 (8th ed. 2016).

120. *See* ARMOUR ET AL., *supra* note 15, at 53 ("The purpose of regulation is to assist markets in functioning better than they would do in its absence. The most important criteria by which economists judge how well an economy is functioning relate to the efficiency with which the economy produces and allocates resources.").

121. *See* John C. Coffee, Jr., *Market Failure and the Economic Case for a Mandatory Disclosure System*, 70 VA. L. REV. 717, 722 (1984).

122. Informational efficiency is seen as important for market fairness as well: Because the securities market is the vehicle for allocating investment capital, "it is important not only that the game be fair, but that it be accurate—that is, that capital be correctly priced." *Id.* at 734. More recently, Professor Ronald Gilson and Professor Reinier Kraakman have expanded this theory in light of the events of the 2008 financial crisis. They argue that information efficiency can lead investors to the "correct" price (what they term "fundamental efficiency"), and that regulation should in fact be designed to "push[] market prices in the direction of fundamental value." Ronald J. Gilson & Reinier Kraakman, *Market Efficiency After the Financial Crisis: It's Still a Matter of Information Costs*, 100 VA. L. REV. 313, 318 (2014); *see generally* Merritt B. Fox et al., *Law, Share Price Accuracy, and Economic Performance: The New Evidence*, 102 MICH. L. REV. 331 (2003) (arguing that to the extent disclosure reduces information asymmetries, disclosure improve price efficiency).

123. *See* Coffee, *supra* note 121, at 722–23, 725.

124. *Id.* at 729. According to Coffee, the idea is that "competition among analysts to 'ferret out and analyze information' maintains market efficiency." *Id.* at 724 n.22.

125. *Id.* at 726.

126. *Id.* at 726–27.

"socially optimal supply of research."[127] As Professor John Coffee has argued along these lines, "[a] mandatory disclosure system can thus be seen as a desirable cost reduction strategy through which society, in effect, subsidizes search costs to secure both a greater quantity of information and a better testing of its accuracy."[128]

A related market failure that mandatory disclosure seeks to address is that of information asymmetries[129] (or the "lemons problem"[130]), which can lead to the problem of "adverse selection." Investors and shareholders know less about a company's risks than a company's managers and directors. Yet shareholders need this kind of information to hold those corporate insiders accountable for protecting their best interests.[131] Likewise, investors need enough information about a company to appraise its value relative to other public companies.[132] Mandatory disclosure can work to level the informational playing field.

Disclosure may also improve corporate governance. As Professor Bob Thompson has argued, disclosure provides directors with information necessary to oversee managers; and, in turn, information with which shareholders can judge the board's ability to monitor the performance of managers and officers.[133] Overall, then, disclosure can empower risk management "watchdogs."[134]

In theory, then, disclosure should provide a mechanism through which market participants and corporate stakeholders exert pressure on the relevant actors to ensure that cyber risk is being well managed. With information about the bank's cyber issues, the market can discipline a company for bad cyber risk management through a drop in share price (or increase in the cost of the bank's debt). Meanwhile, with sufficient information, shareholders can make directors and officers answerable—fireable and compensable—for their cyber risk management prowess.[135]

---

127. *Id.* at 728 ("Put simply, if market forces are inadequate to produce the socially optimal supply of research, then a regulatory response may be justified.").

128. *Id.* at 722.

129. *See* Fox et al., *supra* note 122.

130. Brian R. Cheffins, *Does Law Matter?: The Separation of Ownership and Control in the United Kingdom* 9 (ESRC Ctr. for Bus. Research, Univ. of Cambridge, Working Paper No. 172, 2000), *available at* https://ssrn.com/abstract=245560 [https://perma.cc/J8TE-G4VK] (citing George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488, 489 (1970)).

131. For the classic explication of this problem, see ADOLF A. BERLE, JR. & GARDINER C. MEANS, THE MODERN CORPORATION AND PRIVATE PROPERTY (1932).

132. Cheffins, *supra* note 130, at 10; *see also* ARMOUR ET AL., *supra* note 15, at 55.

133. Robert B. Thompson, *Corporate Governance After Enron*, 40 HOUS. L. REV. 99, 111 (2003); *see also* Mahoney, *supra* note 118, at 1048–50 (discussing the value of disclosure in ameliorating agency costs).

134. Thompson, *supra* note 133, at 111.

135. The potency of these sticks, though, may be weak in the case of cyber risk. *See infra* notes 145–47 and accompanying text.

On that view, the optimal level of cyber disclosure would be such that shareholders and investors could both (1) distinguish among large banks for their proficiency in guarding against cyberattacks, and (2) inform markets whenever a possible loss-occurring cyber event transpired. Accordingly, with both types of information publicly available, the price of bank shares would accurately reflect the value of the bank as discounted by the probability of a successful cyber intrusion multiplied by the magnitude of probable losses incurred by such an attack. And, stated simply, shareholders and directors would know whether managers were doing their jobs to address the cyber risk.

The lack of such specificity in public company disclosure seems to be exactly what is irking the SEC. As we saw in Part III, the banks studied here (like other public companies it seems) have been generic in their disclosures about what measures they are taking to prevent cyber risk, and completely silent about the nature, magnitude, or frequency of actual cyber intrusions. Accordingly, bank cyber disclosures do score poorly against the classic justifications for mandatory disclosure. But in the case of systemically important banks, the value of more information may need to be weighed against financial stability concerns.

2. Operational Resilience as a Public Good

A bank's operational resilience is a public good, too. The public has a strong interest in the uninterrupted provision of the critical economic services that these big banks provide—payments, credit intermediation, and the provision of demand-deposit services.

A cyberattack could threaten any or all of these functions at once.[136] An attack directed to a bank's infrastructure could, for instance, halt its ability to facilitate payments; an attack could also constrict the transfer of credit between financial institutions, or from banks to the real economy—any of these scenarios could bring real economic activity to a crawl or total halt. A cyberattack (of any significant kind) could also be viewed by markets as a serious reputational event, which could incite depositor panic. A cyber attack can also induce a bank's lenders to panic, prompting demands for higher margins on collateral (or the calling in of callable assets). That kind of scenario could lead to serious counterparty losses.[137]

In terms of addressing this kind of financial stability risk, disclosure could cut both ways. Information about a bank's cyber risk management *does* enable the markets to discipline banks that are not sufficiently robust in their cyber

136. Though a discussion of the various ways in which cyber risk presents financial stability risk is beyond the scope of this paper, see, for example, OFFICE FIN. RESEARCH, 2016 FINANCIAL STABILITY REPORT (2016), *available at* https://www.financialresearch.gov/financial-stability-reports/files/OFR_2016_Financial-Stability-Report.pdf [https://perma.cc/LT2R-E52F].

137. *See* Christina Parajon Skinner, *Regulating Nonbanks: A Plan for SIFI Lite*, 105 GEO. L.J. 1379, 1421 (2017).

risk-prevention measures.[138] Capital can then be allocated to those banks that do the 'best' at managing cyber risk (and away from those that are doing poorly). Disclosure thus serves the informational efficiency and accountability goals discussed above, as well as financial stability ones—by supplying the safest banks with the cheapest and most plentiful source of funds.[139] But there are two sides to that coin. Too much disclosure about a cyber issue can undermine confidence in a bank unduly or prematurely.[140] Even more perverse, certain kinds of disclosure can provide a blueprint for would-be cyber attackers to further target the bank. Consequently, the optimal level of bank cyber disclosure would enable beneficial market discipline but stop short of requiring banks to disclose information that would precipitate a loss of confidence.

Arguably, the cyber disclosure rules that apply to this subset of banks should be designed with such balancing principles in mind. The securities law admits this possibility: Section 2 of the 1934 Act notes that the purposes of regulation under the Act include "to protect and make more effective the national banking system."[141] As well, the SEC may, under § 13, authorize —and thus presumably revise—disclosures as "necessary or appropriate for the proper protection of investors."[142] One could interpret § 13 to include protecting investors from the economic harms that result from operational failures at a systemically important bank.

B. SO, WHAT SHOULD BE DISCLOSED?

There are costs and benefits associated with the disclosure of different *types* of cyber disclosures. Recall the typology set out in Part III.

Events. The benefit of requiring banks to disclose cyber events may not outweigh the costs. Although disclosing cyber breaches could allow the market to price the value of a bank's shares more accurately, it could also destroy shareholder value. Take the Equifax disclosure for example. The day

138. *See, e.g.*, Rhiannon Sowerbutts & Peter Zimmerman, *Market Discipline, Public Disclosure and Financial Stability*, *in* THE HANDBOOK OF POST CRISIS FINANCIAL MODELING 42, 42 (Emmanuel Haven et al. eds., 2016) (arguing that debt investors can discipline banks if they have enough disclosures, by withholding funding, and claiming that inadequate disclosure was a contributing factor to the 2008 financial crisis); *see also* Etienne Farvaque, Catherine Refait-Alexandre & Dhafer Saidane, *Corporate Disclosure: A Review of its (Direct and Indirect) Benefits*, 128 DANS ÉCONOMIE INTERNATIONALE 5, 30 (2011).

139. *See* Report of the Advisory Committee on Corporate Disclosure to the Securities and Exchange Commission, H.R. REP. 98-910, vol. 1, at XVI (1977) (noting "that the most efficient allocation of resources will occur when the information is sufficient for the purposes of those making decisions, when it is reliable, and when it is disseminated in a timely manner").

140. As others have noted, "[i]n the immediate aftermath of a major breach, the 'known' facts may represent a small piece of the cybersecurity risk mosaic." Dembosky & Feigelson, *supra* note 72.

141. 15 U.S.C. § 78b (2012).

142. *Id.* § 78m(a).

following its announcement, the share price dropped 13.7%.[143] Imagine if that disclosure had been forced by regulators prematurely and was inaccurate as a result.[144] That loss of value would not be efficient. In the same vein, disclosing cyber incidents could be taken by the market as a sign of the bank's weakness, resulting in the loss of customers, higher margin calls by creditors, or higher spreads on debt that the bank seeks in the interbank or short-term funding markets. All of these outcomes would be bad for existing shareholders. And if the information were inaccurate, it would distort—not facilitate—price efficiency.

It is also unclear whether corporate accountability would improve from event-based disclosure. After all, where a breach has already transpired, it is too late for shareholders to press boards and managers for more attentive cyber risk management. Directors or managers could be fired or have their compensation docked as 'punishment'; but such deterrents might be redundant. Unlike a decision to take risks with investments—where reasonable minds can differ about the proper limits of risk-taking —cyber risk is universally acknowledged as a negative risk to the business. No one seeks it out. Accordingly, managers and boards likely are already incentivized to bring that risk as close to zero as is privately cost effective. And if banks are underinvesting in cyber defense resources—that is, at a level that is privately cost effective but beneath the social optimum—procedural and investment-oriented disclosure might be more effective in guiding the market's discipline.[145]

On the financial stability side of the ledger, it is nearly impossible to see any gains from disclosing cyber events. At best, that kind of information would be neutral for stability; at worst, it would undermine confidence in the institution, which in turn could become contagious and market-freezing. Equally damaging, disclosing an open breach could invite further attacks on the institutions that might be more damaging than the last.

On balance, then, it seems that the costs outweigh the benefits of requiring event-based disclosure. Going further, this analysis may suggest that "materiality" is even too low a bar for requiring cyber event disclosure.[146] The

143. *See* Elizabeth Weise, *A Timeline of Events Surrounding the Equifax Data Breach*, USA TODAY (Oct. 3, 2017, 2:46 PM), https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001[https://perma.cc/YZ9T-TSJU].

144. As others have noted, "in the immediate aftermath of a major breach, the 'known' facts may represent a small piece of the cybersecurity risk mosaic." Dembosky & Feigelson, *supra* note 72.

145. Lucian A. Bebchuck & Holger Spamann, *Regulating Bankers' Pay*, 98 GEO. L.J. 247, 282–85 (2010); Steven L. Schwarcz, *Misalignment: Corporate Risk-Taking and Public Duty*, 92 NOTRE DAME L. REV 1, 16–22 (2016); *see Skinner*, *supra* note 137, at 1417–18; *see also, e.g.*, John Armour & Jeffrey N. Gordon, *Systemic Harms and Shareholder Value*, 6 J. LEGAL ANALYSIS 35, 58 (2014). As such, market discipline does play an important role, but perhaps not for events.

146. The Guidance states:

> The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised

2018 SEC Cyber Guidance draws from decades-old Supreme Court precedent when stating that information is material for disclosure purposes "if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision" or if the information would "significantly alter[] the total mix of information made available."[147] Yet, as just discussed, what information would be relevant to an investment decision is only partially representative of the public interests at stake in bank cyber disclosure.

Procedures and Investments. On the other hand, the SEC may be warranted in requesting more extensive disclosures about the procedural steps that banks are taking to fortify themselves against cyber risk. In particular, as alluded to above, mandating disclosure might be necessary to ensure that banks are investing the socially optimal amount of resources in their cyber defenses. It may well be that banks are incentivized to invest in cyber defenses at the level that is privately cost effective, but not sufficiently expansive in light of the various social and macro interests in play.[148] This is not just a cyber issue; companies can often be expected to underinvest in a socially beneficial piece of infrastructure or technology that is designed to mitigate a negative externality.[149] Accordingly, it may justifiable for the SEC to set more rigorous disclosure requirements regarding the preventative and investment-related efforts that banks are taking to mitigate their cyber risk.

As we saw in Part III, banks' disclosures on these topics may still be too general and generic. The SEC's 2018 cyber guidance made clear that it "expect[s] companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents."[150] And "[c]ompanies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors."[151] So, clearer or firmer guidelines may still be needed. But again, financial stability interests should set the outer limit. While it would be reasonable to press banks to be more specific and differentiated in their

> information or the business and scope of company operations. The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-US authorities.

SEC Cyber Guidance, supra note 4, at 11 (footnotes omitted).

147. *Id.* at 10 (quoting TSC Industries v. Northway, 426 U.S. 438, 449 (1976)).

148. *See* WHITE HOUSE REPORT, *supra* note 3, at 25 ("[F]irms will choose their optimal level of investment by conducting an analysis of private costs . . . . In light of this market failure, regulators can devise a scheme of penalties and incentives that are designed . . . [to] raise levels of cybersecurity investment to the socially optimal level.").

149. ARMOUR ET AL., *supra* note 15, at 57.

150. *SEC Cyber Guidance, supra* note 4, at 13.

151. *Id.* at 13.

disclosures about cyber risk management procedures and controls, banks should not be pushed to outline how best to storm the fort.

C. TO WHOM SHOULD BANKS DISCLOSE?

To be clear, while this Part has argued that the costs of requiring *public* disclosure of cyber events may be unreasonable, this is *not* to say that banks should keep such information completely hidden from external view.

There are semi-public modes of disclosing events that the SEC may wish to consider. For example, under the European Union General Data Protection Regulation ("GDPR"), which took effect in May 2018, an organization is required to notify its national data protection authority of any breach within 72 hours of becoming aware of it.[152] A breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data."[153] The GDPR Guidelines add that this includes "even" temporary loss or unavailability of the personal data.[154] At a very high level, the GDPR regime models one way of disclosing breaches (material or otherwise) to whichever regulator is best positioned to work with the industry to remedy the problem.

There are also private industry bodies to whom disclosure might be made. ORX is a prime example. ORX is a private, opt-in membership-based organization that helps the global banking and insurance industry share loss data.[155] The idea behind ORX is that by sharing loss data, banks can better understand the kind of operational risk facing their peer institutions, even if the institution-identifying information is anonymized. This kind of loss-pooling system could help banks predict the magnitude of cyber events based on recent precedent and current cases. Moreover, in providing a platform for sharing loss data, ORX can also position itself to have convening power. A third party like ORX can bring institutions together to collate and share best practices for cyber risk management. In turn, were banks to disclose the fact of their participation in ORX, for example, that might provide a kind of procedural datapoint that markets and investors would find valuable, with

---

152. *See generally* Council Regulation 2016/679, General Data Protection Regulation, art. 33 cl. 1, 2016 O.J. (L 119/52) (proscribing a new data protection regime applicable to the European Union and setting a 72-hour notification window for personal data breaches).

153. *Id.* at art. 4 cl. 12, 119/34.

154. *See* ARTICLE 29 WORKING PARTY, GUIDELINES ON PERSONAL DATA BREACH NOTIFICATION UNDER REGULATION 2016/679, at 7 (2017), *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 [https://perma.cc/E76A-NB7U]; *see also* Colin Pearson & Xuyang Zhu, *Notification of Data Breaches Under the GDPR—10 Frequently Asked Questions*, CLEARY GOTTLIEB: CLEARY CYBERSECURITY & PRIVACY WATCH (Jan. 18, 2018), https://www.clearycyberwatch.com/2018/01/notification-data-breaches-gdpr-10-frequently-asked-questions [https://perma.cc/3VG2-L2BV].

155. "ORX was founded with a vision of creating a platform for the anonymised and secure exchange of high-quality loss data relating to operational risk." *ORX Loss Data*, O.R.X., https://managingrisktogether.orx.org/activities/loss-data [https://perma.cc/V96W-J3DB].

little corresponding cost to financial stability. The SEC may also wish to consider whether requiring (or guiding) banks to participate in private loss-sharing consortia is one viable way of fulfilling their mandate to design disclosure rules that "make" the national banking system effective.[156]

V. THE LIMITS OF DISCLOSURE AND SYSTEMIC CYBER RISK

Until this point, the Article has urged the architects of mandatory disclosure rules to bear financial stability goals in mind, where those rules apply to certain banks. But it is quite another matter to suggest that disclosure is a tool that is sufficient to address the financial stability risks associated with G-SIB cyber risk. Disclosure, after all, is not ideally suited to *prevention*. Consequently, certain gaps in G-SIB regulation will inevitably remain, even assuming an optimally designed disclosure regime. Although future work will address this subject in fuller depth, this Part briefly previews these gaps in cyber regulation, which disclosure is not and cannot be designed to fill.

Scholars of regulatory design have long debated the merits of disclosure-based versus direct regulation for addressing market failures.[157] In financial markets, those that view disclosure as preferable to direct regulation do so on the view that the economic actors participating in capital markets—not regulators—should be the ones to make substantive decisions about the "quality" of securities.[158] This rationale fits naturally with the informational efficiency and accountability justifications of mandatory disclosure.

Disclosure can partially serve financial stability goals. As discussed above, mandatory disclosure can incentivize banks to invest in cyber defense resources beyond what is privately cost effective, at levels closer to the social optimum (assuming such a resource gap exists). Still, market discipline can only go so far. After all, the market might undervalue the cyber risk at hand or overvalue banks' cyber risk mitigation efforts. Because the nature of cyber risk is relatively opaque, amorphous, and stems from a range of different actors, the likelihood of socially costly error here is high. But perhaps even more importantly, disclosure does not set specific standards for or coordinate the banks' approaches to combatting cyber risk. There are other regulatory tools available for such purpose.

The Dodd-Frank Act equipped bank regulators with an innovative arsenal of tools for maintaining the stability of the entire financial system.[159] The

156. *See* 15 U.S.C. § 78b (2012).

157. Douglas A. Kysar, *Preferences for Processes: The Process/Product Distinction and the Regulation of Consumer Choice*, 118 HARV. L. REV. 526, 527 (2004); *see, e.g.*, STEPHEN BREYER, REGULATION AND ITS REFORM 163 (1982).

158. *See* Paula J. Dalley, *The Use and Misuse of Disclosure as a Regulatory* System, 34 FLA. ST. U. L. REV. 1089, 1098 (2007).

159. *See generally* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 165, 124 Stat. 1376 (2010) (providing regulators several tools or methodologies to ensure banks' resiliency).

challenge going forward, however, is that these tools were not designed to address nonfinancial risks like cyber risk. So some re-fitting may be needed. Stress testing is one example. Regulatory stress tests involve scenario-based planning.[160] These tests involve a regulator-posed scenario—of some adverse or extremely adverse economic event—to which banks must respond by demonstrating how they would remain solvent and within regulatory capital limits. (In the United States, the Fed conducts a supervisory stress test, formally called the "Comprehensive Capital Analysis and Review" ("CCAR"), on large American bank holding companies and foreign bank subsidiaries.)[161]

But capital would be of little use in quelling panic in the event that a cyber-attack prevented the withdrawal of cash deposits or a freeze of the interbank payments system. These are fundamentally operational issues that require an operational—not balance-sheet—focused simulation. Some innovation here is happening. Regulators in several EU jurisdictions, for example, subject their banks to penetration testing. The banks will "test" information security controls in relation to hardware, software, and data as to how well those controls perform to prevent, detect, respond, and recover from cyber-incidents.[162] The bank supervisors then "review and challenge" the bank's approach to testing and require remediation if needed.[163]

Recovery planning is another tool ripe for revisiting in light of cyber risk.[164] The motivation behind recovery planning stems from the crisis-learned lesson that banks must have "plans" for "identifying and responding

160. *See* BASEL COMM. ON BANKING SUPERVISION, PRINCIPLES FOR SOUND STRESS TESTING PRACTICES AND SUPERVISION (2009) (providing guidance for banks' stress testing practices); *see also* Mehrsa Baradaran, *Regulation by Hypothetical*, 67 VAND. L. REV. 1247, 1283–88 (providing a history of stress testing); *Dodd-Frank Act Stress Test (Company-Run)*, OFF. COMPTROLLER CURRENCY, http://www.occ.gov/tools-forms/forms/bank-operations/stress-test-reporting.html [https://perma.cc/4UQZ-AJVP].

161. In the United States, the first stress test (the Supervisory Capital Assessment Program) was conducted on 19 U.S.-owned bank holding companies in 2009. BEVERLY HIRTLE & ANDREAS LEHNERT, FED. RESERVE BANK OF N.Y., STAFF REPORT NO. 696, SUPERVISORY STRESS TESTS 9 (2014), *available at* https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr696.pdf [https://perma.cc/79BK-U5KP]. Comprehensive Capital Analysis and Review ("CCAR"), now an annual exercise, began in 2011. *Id.* at 16. The 2014 CCAR tested 30 bank holding companies with assets of at least $50 billion. *Id.*

162. BASEL, CYBER-RESILIENCE , *supra* note 20, at 18.

163. *Id.* Five EU jurisdictions have developed regulator-led penetration tests, while the ECB, the Netherlands, and the U.K. have also developed guidance for institutions on how to conduct a test.

164. OCC Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches, Technical Amendments, 81 Fed. Reg. 66,791, 66,791–801 (Sept. 29, 2016), *amended by* OCC Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches, 83 Fed. Reg. 66,604, 66,604–07 (Jan. 28, 2019). The Guidelines are enforceable pursuant to § 39 of the Federal Deposit Insurance Act. Federal Deposit Insurance Act § 39, 12 U.S.C. § 1831p-1(e) (2012).

rapidly to significant stress events."[165] OCC guidelines require banks to identify "triggers" that could put the institution in distress. Unlike stress testing where the regulator designs the stress scenario, banks are required to construct and respond to their own bespoke scenario when preparing a recovery plan.[166]

As professional services experts have advised, the scenarios banks choose should reflect the bank's unique set of "vulnerabilities" based on its mix of business activities.[167] The law firm Covington & Burling and auditors Ernst & Young, for example, advised their financial institution clients that banks might plan for an "operational event" that might result in several financial losses, like a cyber attack.[168]

Recovery planning is still in its inception. For those banks with $50 billion or more in assets, the first plans were due July 1, 2018.[169] So there are only one set of plans to consider in assessing banks' recovery planning behavior. While the recovery plans are not public, so one cannot know for sure, there may be reason to assume that cyber has not, so far, been included—that is, by looking for clues in banks resolution plans.[170]

The OCC Guidelines require banks to integrate their recovery plans with their capital plans, stress testing documents, and resolution plans.[171] Doing so makes sense for the business of the bank, given that banks are constantly operating along some "continuum" of 'business as usual' to resolution—so banks may be drawing from resolution plans in creating their recovery plans.[172] However, cyber issues did not appear in the public portion of the

165. *OCC Bulletin 2016-30: Enforceable Guidelines for Recovery Planning: Final Guidelines*, OCC (Sept. 29, 2016), https://www.occ.treas.gov/news-issuances/bulletins/2016/bulletin-2016-30.html [https://perma.cc/89VL-CQTK].

166. *See generally* COVINGTON & EY, THE OCC'S FINAL GUIDANCE FOR RECOVERY PLANNING: GETTING STARTED GUIDE (Feb. 2017), *available at* https://www.cov.com/-/media/files/corporate/publications/2017/02/the_occs_final_guidance_for_recovery_planning.pdf [https://perma.cc/FG89-DLWB].

167. *Id.* at 10.

168. *Id.*

169. OCC Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches, Technical Amendments, 81 Fed. Reg. at 66,793 (calculating that 18 months after the rule's effective date of January 1, 2017 is July 1, 2018).

170. Section 165(d) of the Dodd-Frank Act required banks to prepare resolution plans, commonly known as "living wills." These plans are meant to describe the company's plan for orderly resolution in the event the bank suffers "material financial distress" or failure. *See Living Wills (or Resolution Plans)*, BD. GOVERNORS FED. RESERVE SYS. (July 2, 2019), https://www.federalreserve.gov/supervisionreg/resolution-plans.htm [https://perma.cc/5FNA-ZTFT].

171. *See* COVINGTON & EY, THE OCC'S FINAL GUIDANCE FOR RECOVERY PLANNING, *supra* note 166, at 8.

172. *See id.* at 15 (noting that there is no regulatory requirement for the scenarios to mirror one another, but it makes good business sense for them to do so).

plans submitted by many of the banks studied here.[173] Goldman Sachs mentions it only in connection with its Firmwide Technology Risk Committee.[174] Wells Fargo did give some mention in its plan to modifications in its governance structure from years prior.[175] The enhancements it submitted were "designed to allow for rapid execution of Board of Directors and senior management actions during stress events . . . . [and] risk-agnostic to allow for comprehensive response to any type of risk event (e.g., cyber threat, natural disaster, financial stress)."[176] It is encouraging to see cyber acknowledged as a possible cause of the bank's stress, though the remarks seem meant to provide context to Wells Fargo's efforts to shore up its risk management; they do not necessarily suggest the bank is preparing a cyber-focused stress scenario.

The recovery planning framework, as well as stress testing, are recent additions to banking regulation. Their objectives and design are still capable of amending, provided policymakers and regulators have the will to innovate further.[177] And banks have all the runway that they need to integrate cyber scenarios into their recovery planning. They may soon voluntarily do so, recognizing the heightened risk of cyber exposure; if not, expansion may be prodded by further OCC guidelines requiring banks to add cyber triggers to their plans for supervisors to review.

---

173. CITIGROUP INC., 2017 RESOLUTION PLAN: PUBLIC SECTION (2017), *available at* https://www.fdic.gov/regulations/reform/resplans/plans/citi-165-1707.pdf [https://perma.cc/7YLQ-AXE7]; JPMORGAN CHASE & CO., 2017 RESOLUTION PLAN PUBLIC FILING (2017), *available at* https://www.federalreserve.gov/supervisionreg/resolution-plans/jpmorgan-chase-1g-20170701.pdf [https://perma.cc/Y6CB-TESN]; *see, e.g.*, BANK OF AM. CORP., 2017 RESOLUTION PLAN SUBMISSION: PUBLIC EXECUTIVE SUMMARY (2017), *available at* https://www.federalreserve.gov/supervisionreg/resolution-plans/boa-1g-20170701.pdf [https://perma.cc/K9MR-Z8H3] (not mentioning cyber issues).

174. GOLDMAN SACHS GRP. INC., 2017 RESOLUTION PLAN: PUBLIC SECTION 114 (2017), *available at* https://www.federalreserve.gov/supervisionreg/resolution-plans/goldman-sachs-1g-20170701.pdf [https://perma.cc/TVQ9-YUVU].

175. *See* Laura J. Keller, *Wells Fargo Boosts Fake-Account Estimate 67% to 3.5 Million*, BLOOMBERG (Aug. 31, 2017, 3:05 PM), https://www.bloomberg.com/news/articles/2017-08-31/wells-fargo-increases-fake-account-estimate-67-to-3-5-million [https://perma.cc/J9HW-83F7]; *see also* Jabbari v. Wells Fargo & Co., No:15-cv-02159-VC, 2017 WL 5157608, at *10–15 (N.D. Cal. July 8, 2017).

176. WELLS FARGO, 2017 RESOLUTION PLAN: PUBLIC Section 21 (2017), *available at* https://www.fdic.gov/regulations/reform/resplans/plans/wellsfargo-165-1707.pdf.

177. *See* Randal K. Quarles, Vice Chairman for Supervision, Bd. of Gov. of the Fed. Reserve Sys., Speech at the Brookings Institution, Washington, D.C.: A New Chapter in Stress Testing (Nov. 9, 2018), *available at* https://www.federalreserve.gov/newsevents/speech/quarles20181109a.htm (publicly stating that "our stress testing regime—like the banking and financial system that it evaluates—will and should evolve as we continue to learn from experience in the management of this tool").

VI. CONCLUSION

By reviewing nearly 900 SEC filings from the seven systemically important U.S. banks, this Article has provided comprehensive evidence about what and how banks disclose their cyber issues. Assessing the content of these disclosures against three separate regulatory goals—information efficiency, board and manager accountability, and financial stability—the Article suggested some flaws in the design of the SEC's current cyber disclosure guidance. In particular, rules or guidance condoning less (if any) cyber event disclosure, but requiring more procedural and investment related disclosure, would be more likely to maximize the various private and public interests at stake. The Article also previewed the outer limits of disclosure as a tool for mitigating systemic cyber risk: Insofar as disclosure cannot prevent cyber risk from destabilizing the financial system, bank regulators will need to revise and deploy certain post-crisis tools to fill in the gaps.