CYBER BABEL: FINDING THE LINGUA FRANCA IN CYBERSECURITY REGULATION

*William Pierotti**

Cybersecurity regulations have proliferated over the past few years as the significance of the threat has drawn more attention. With breaches making headlines, the public and their representatives are imposing requirements on those that hold sensitive data with renewed vigor. As high-value targets that hold large amounts of sensitive data, financial institutions are among the most heavily regulated. Regulations are necessary. However, regulations also come with costs that impact both large and small companies, their customers, and local, national, and international economies. As the regulations have proliferated so have those costs. The regulations will inevitably and justifiably diverge where different governments view the needs of their citizens differently. However, that should not prevent regulators from recognizing areas of agreement.

This Note examines the regulatory regimes governing the data and cybersecurity practices of financial institutions implemented by the Securities and Exchange Commission, the New York Department of Financial Services, and the General Data Protection Regulations of the European Union to identify areas where requirements overlap, with the goal of suggesting implementations that promote consistency, clarity, and cost reduction.

* J.D. Candidate, 2019, Fordham University School of Law; B.A., 2011, Moravian College. I would like to thank Professor Joel R. Reidenberg for extending his experience and thoughtful guidance throughout this process. I would also like to thank my family and friends for their unwavering support and the editors and staff of the *Fordham Law Review* for their assistance.

INTRODUCTION

My name is Legion: for we are many.

—Mark 5:9[1]

After Yahoo! disclosed two cyberbreaches, Verizon lowered its offer to purchase Yahoo! by $350 million—from $4.83 billion to $4.48 billion.[2] This represented a 7 percent decrease in value. With over one billion compromised accounts, the Yahoo! breach was massive.[3] It is significant, however, that the compromised information took the form of email addresses, names, telephone numbers, and dates of birth.[4] The Equifax breach affected roughly 143 million Americans, and the data exposed arguably included more sensitive information, such as Social Security and credit card numbers.[5] While the ultimate outcome of the Equifax breach remains uncertain and the company has regained some of its lost value,[6] the

1. *Mark* 5:9 (King James).

2. Ingrid Lunden, *After Data Breaches, Verizon Knocks $350M Off Yahoo Sale, Now Valued at $4.48B*, TECHCRUNCH (Feb. 21, 2017), https://techcrunch.com/2017/02/21/verizon-knocks-350m-off-yahoo-sale-after-data-breaches-now-valued-at-4-48b/ [https://perma.cc/5YVL-MF3F].

3. *Id.*

4. Kate Conger, *Yahoo Discloses Hack of 1 Billion Accounts*, TECHCRUNCH (Dec. 14, 2016), https://techcrunch.com/2016/12/14/yahoo-discloses-hack-of-1-billion-accounts/ [https://perma.cc/AZ75-ESB7].

5. Michelle Fox, *Equifax Will Not Survive Fallout from Massive Breach, Says Technology Attorney*, CNBC (Sept. 14, 2017, 7:01 PM), https://www.cnbc.com/2017/09/14/equifax-will-not-survive-fallout-from-massive-breach-says-technology-attorney.html [https://perma.cc/YVE5-CLGV].

6. Wayne Duggan, *Equifax Stock May Be OK, After All*, U.S. NEWS (Nov. 10, 2017, 7:17 AM), https://money.usnews.com/investing/stock-market-news/articles/2017-11-10/equifax-inc-efx-stock-earnings-data-breach [https://perma.cc/EYR5-47YX].

initial market loss was $4 billion.[7] That represents a 20 percent decrease in market value.[8] The actual costs of the breach, even if the stock regains value and after insurance coverage kicks in, have been estimated at $200 to $300 million.[9]

Breaches[10] represent a significant threat to businesses and consumers.[11] Businesses that hold sensitive information about their consumers, such as financial institutions, make tempting targets for cybercriminals.[12] The cost of a breach, per record lost or stolen, at a financial institution is also higher than in most other industries.[13] Because these institutions need to remain connected to the internet, it is likely impossible for them to fully prevent intrusions.[14] Given this reality, the focus has been on what should be required of these institutions to limit the risk, mitigate the damage, and notify their consumers.[15]

As a result of the importance of the issue and the multijurisdictional significance of these institutions, a number of government organizations and agencies have addressed these questions.[16] While goals are similar,

---

7. Paul J. Lim, *Equifax's Massive Data Breach Has Cost the Company $4 Billion So Far*, TIME (Sept. 12, 2017), http://time.com/money/4936732/equifaxs-massive-data-breach-has-cost-the-company-4-billion-so-far/ [https://perma.cc/M97T-5WTN].

8. *Id.*

9. *Id.*

10. PONEMON INST., 2017 COST OF DATA BREACH STUDY: GLOBAL OVERVIEW 7 (June 2017), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN [https://perma.cc/BM6D-RWXQ] (defining a breach "as an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk—either in electronic or paper format").

11. *See* Stacy Cowley, *FBI Director: Cybercrime Will Eclipse Terrorism*, CNN (Mar. 2, 2012, 7:55 AM), http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/ [https://perma.cc/YS59-AFK4]; Stephanie Palmer-Derrien, *"No Greater Threat" Than Cyber, Says SIFMA*, ASSETSERVICINGTIMES (Nov. 2, 2017), http://www.assetservicingtimes.com/assetservicesnews/article.php?article_id=7741 [https://perma.cc/RFK5-J5QC] ("Testifying before the US House of Representatives committee on financial services subcommittee hearing on data security, [president and CEO of the Securities Industry and Financial Markets Association Kenneth] Bentsen said: 'There is likely no greater threat to financial stability than a large-scale cyber event.'").

12. Palmer-Derrien, *supra* note 11; Larry Zelvin, Director, Nat'l Cybersecurity & Commc'ns Integration Ctr., U.S. Dep't of Homeland Sec., Remarks at U.S. Securities and Exchange Commission Cybersecurity Roundtable 28 (Mar. 26, 2014), https://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt [https://perma.cc/A6JL-Y46R].

13. PONEMON INST., *supra* note 10, at 5 ("Certain industries have more costly data breaches. The average global cost of data breach per lost or stolen record was $141. However, health care organizations had an average cost of $380 and in financial services the average cost was $245.").

14. *See generally* Cowley, *supra* note 11 ("There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again . . . .").

15. Bhashit (Sheek) Shah, *SEC Increases Focus on Cyber Incident Response*, REED SMITH LLP (Aug. 6, 2017), https://www.technologylawdispatch.com/2017/08/privacy-data-protection/sec-increases-focus-on-cyber-incident-response/ [http://perma.cc/7Y3Z-PMUB].

16. *Id.*

implementations have varied.[17] These variations could unintentionally divert resources from expenditures on security towards understanding and administering compliance programs.[18] Industry representatives emphasize the importance of cybersecurity in the financial sector.[19] However, they also present a troubling figure, with firms "report[ing] that approximately 40 percent of corporate cybersecurity activities are compliance-oriented rather than security-oriented."[20] Regulatory bodies could mitigate this issue by acknowledging areas of overlap and working together to define common standards.[21] Currently, each covered entity must perform this analysis independently at substantial cost, regardless of size or availability of resources, with limited exceptions.[22] Regulatory bodies should diminish areas of uncertainty and facilitate more efficient allocations of resources by identifying and aligning similar requirements.

This is particularly important with regard to financial institutions, as they are part of the critical infrastructure of the United States[23] and the European Union (EU).[24] In the United States, critical infrastructure has been defined as systems that are so vital to the United States that their "incapacity or destruction . . . would have a debilitating impact on security, national

17. *See generally* Allison Grande, *Cybersecurity Policy to Watch for the Rest of 2017*, LAW360 (July 12, 2017, 7:47 PM), https://www.law360.com/articles/937323/cybersecurity-policy-to-watch-for-the-rest-of-2017 [https://perma.cc/8PJ2-PZWJ].

18. Palmer-Derrien, *supra* note 11; *see also* Michael Krimminger et al., *New York Cybersecurity Regulations for Financial Institutions Enter into Effect*, CLEARY GOTTLIEB STEEN & HAMILTON LLP (Mar. 3, 2017), https://www.clearygottlieb.com/-/media/organize-archive/cgsh/files/publication-pdfs/alert-memos/alert-memo-201729.pdf [https://perma.cc/JQ8W-5S4L].

19. Securities Industry and Financial Markets Association et al., Comment Letter on New York Department of Financial Services' Proposed Rulemaking on Cybersecurity Requirements for Financial Services Companies 2 (Nov. 14, 2016) [hereinafter SIFMA Comment Letter], https://www.aba.com/Advocacy/commentletters/Documents/SIFMA-NY-DFS-Proposed-Cyber-Requirements.pdf [http://perma.cc/4YXA-97KF] (stating that "[c]ybersecurity remains a top priority for the financial industry," with "investments that can run as high as $500 million per year for the largest firms"); *see also* Bhargav Mitra & Robert McCausland, *How Identity Data Is Turning Toxic for Big Companies*, CONVERSATION (Dec. 4, 2017, 4:05 AM), https://theconversation.com/how-identity-data-is-turning-toxic-for-big-companies-88436 [http://perma.cc/JAY5-E5WP] ("One report has found that banks spent nearly US$100 billion on compliance in 2016 and the global spending on meeting the regulatory requirements increased from 15% to 25% over the previous four years. This skyrocketing spend on compliance leaves little room for product development.").

20. SIFMA Comment Letter, *supra* note 19, at 2.

21. *See generally* PRIVACY BRIDGES: EU AND US PRIVACY EXPERTS IN SEARCH OF TRANSATLANTIC PRIVACY SOLUTIONS (2015) [hereinafter PRIVACY BRIDGES], https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf [http://perma.cc/46CS-MY33].

22. *See* Mitra & McCausland, *supra* note 19 ("[P]urchasing the technology to adhere to the GDPR standards . . . will cost Fortune 500 companies on average US$1m each. Add to this the costs of permanent staffing and legal advice for this compliance, you get the picture of overall spending required for one set of regulatory standards.").

23. 42 U.S.C. § 5195c (2012).

24. European Commission Memorandum MEMO/06/477, European Programme for Critical Infrastructure Protection (Dec. 12, 2006).

economic security, national public health or safety."[25] Similarly, the EU has defined them as systems that are "essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people" such that there would be a significant impact if they were destroyed or degraded.[26] Given the significance of the financial sector, it is crucial to regulate in a way that furthers the enunciated security goals as effectively as possible. Compliance with cybersecurity regulations should promote better cybersecurity, not unnecessary expenditures on understanding byzantine regulatory regimes. Clarifying where the myriad and opaque obligations created by various regulatory schemes overlap and can be satisfied through a single action or process would help accomplish this extremely important goal and would also ensure that resources are actually used to improve cybersecurity. The regulatory bodies that propagated those regulations are best situated to do so.

This Note examines three bodies charged with regulating in this area: the Securities and Exchange Commission (SEC), New York Department of Financial Services (NYDFS), and EU. Part I provides an overview of the current regulatory landscape. Part II identifies similar or associated requirements that provide an opportunity for standardization or clarification. Part III explores the benefits of coordination, recommends mechanisms the regulatory bodies could use to coordinate, and applies them to the areas identified in Part II.

I. THE CURRENT CYBERSECURITY REGULATORY LANDSCAPE

Part I of this Note provides a baseline explanation of which entities are affected by each regulatory regime, how the regulations developed, what compliance with the regulations entails, and a discussion of what some of the potential ramifications of the regulations are. Part I.A discusses the regulations, guidance, and other materials that have been disseminated by three regulatory bodies, the SEC, NYDFS, and EU, to determine what measures they expect covered entities to take. Part I.B explores the costs of compliance, providing insights into the effects these regulations have and current trends in the financial industry that may be influenced by these regulations.

A. Where We Are in Cyberregulation and How We Got Here

Part I.A provides an outline of the three regulatory regimes, particularly regarding their jurisdiction, evolution, and a broad explanation of their requirements. Part I.A begins with the SEC requirements, proceeds to the NYDFS regulations, and concludes with the EU's General Data Protection Regulation (GDPR).

25. 42 U.S.C. § 5195c(e).
26. Council Directive 2008/114, art. 2, 2008 O.J. (L 345) 75, 77 (EC).

1. Putting the SEC in Security

On November 13, 2000, the SEC's "safeguards rule," which established appropriate standards for the protection of customer information at financial institutions, came into effect.[27] Since the SEC has jurisdiction over investment advisers,[28] brokers,[29] dealers,[30] and investment companies,[31] all entities that are characterized as such are subject to the safeguards rule.[32] Further, any financial institutions that engage in these activities, such as some banks, must evaluate whether they are subject to the SEC's jurisdiction and, if so, must comply with this regulation.[33]

In 2005 the safeguards rule was updated to require covered entities to create and implement "written policies and procedures" that contemplate "administrative, technical, and physical safeguards" for the purposes of protecting customer information.[34] These policies must be "reasonably designed" to accomplish three goals with regard to customer data: (1) provide for the data's security and confidentiality; (2) protect the data from anticipated threats; and (3) prevent unauthorized access to or use of the data that could cause substantial harm or inconvenience.[35]

For a decade after promulgating these regulations, the SEC only brought three enforcement actions based on the cybersecurity measures implemented by covered entities. The first enforcement action was brought against the LPL Financial Corporation after it suffered a breach that resulted in third-party trading and attempts to trade on several customer accounts.[36] In this action, the SEC established that written policies must be sufficient.[37] The SEC stated that LPL's written policies were limited, insufficient, and failed to address the administrative, technical, and physical safeguards discussed above.[38] The SEC also noted that LPL disregarded the regulatory

27. 17 C.F.R. § 248.18(a) (2018).

28. STAFF OF THE INV. ADVISER REGULATION OFFICE DIV. OF INV. MGMT., U.S. SEC. & EXCH. COMM'N, REGULATION OF INVESTMENT ADVISERS BY THE U.S. SECURITIES AND EXCHANGE COMMISSION 1 (2013), https://www.sec.gov/about/offices/oia/oia_investman/rplaze-042012.pdf [http://perma.cc/R2BG-GATQ] (defining investment advisers to include "[m]oney managers, investment consultants, and financial planners").

29. 15 U.S.C. § 78c(a)(4)(A) (2012) (defining brokers to include individuals who professionally effect securities transactions on behalf of others).

30. *Id.* § 78c(a)(5)(A) (defining dealers to include individuals who professionally buy or sell securities on their own behalf).

31. 15 U.S.C. § 80a-3(a)(1)(A) (2012) (defining an investment company as an issuer that "is or holds itself out as being engaged primarily, or proposes to engage primarily, in the business of investing, reinvesting, or trading in securities").

32. 17 C.F.R. § 248.1(b).

33. *Guide to Broker-Dealer Registration*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/reportspubs/investor-publications/divisionsmarketregbdguidehtm.html [http://perma.cc/CDK2-28AA] (last modified Dec. 12, 2016) ("[B]anks that buy and sell securities must consider whether they are 'dealers' under the federal securities laws.").

34. 17 C.F.R. § 248.30(a).

35. *Id.*

36. LPL Fin. Corp., Exchange Act Release No. 58,515, Investment Advisers Act Release No. 2775, at 3 (Sept. 11, 2008).

37. *Id.* at 4.

38. *Id.*

requirements by failing to take action when alerted to possible security issues.[39]

The SEC's second enforcement action was brought against Commonwealth Equity Services after intruders accessed its intranet and acquired a list of its customers' accounts.[40] The intruders subsequently used eight compromised customer accounts to place orders before the activity was detected.[41] The SEC found Commonwealth's security procedures inadequate, despite the company's written policies that addressed administrative, technical, and physical safeguards.[42] The SEC noted the failure to employ basic safeguards, such as installing antivirus software on all computers connected to the internet.[43] The SEC also emphasized the failure to address, or have a procedure to handle, security issues that were discovered through either audits or reports to the IT help desk.[44] These weaknesses demonstrated that the policy was not reasonably designed as required.[45]

The third enforcement action was brought against GunnAllen Financial after three laptop computers and an employee's computer credentials were stolen, which put customer information at risk.[46] The SEC found that the company's written policy was insufficient because it failed to define specific procedures and safeguards that would be implemented.[47] The SEC also noted the absence of staff guidance explaining their role in protecting customer information and complying with the safeguards rule.[48] Similar to the action against Commonwealth, the SEC noted the absence of procedures for rectifying potential security issues and for responding to a breach.[49]

Despite a relatively slow start, "[r]ecent enforcement actions targeting violations of the safeguards rule show that the SEC is serious about cybersecurity compliance."[50] Since 2015, the SEC has settled enforcement actions against three entities for failing to comply with the safeguards rule

39. *Id.* at 5.

40. Commonwealth Equity Servs., LLP, Exchange Act Release No. 60,733, Investment Advisers Act Release No. 2929, at 3 (Sept. 29, 2009).

41. *Id.*

42. *Id.* at 4.

43. *Id.*

44. *Id.* at 4–5.

45. *Id.* at 5.

46. Marc A. Ellis, Exchange Act Release No. 64,220, at 2 (Apr. 7, 2011).

47. *Id.* at 3.

48. *Id.* at 5.

49. *Id.*

50. Rajesh De et al., *New Heads of Enforcement at the US Securities and Exchange Commission Continue Agency's Focus on Cybersecurity*, MAYER BROWN (July 12, 2017), https://www.mayerbrown.com/New-Heads-of-Enforcement-at-the-US-Securities-and-Exchange-Commission-Continue-Agencys-Focus-on-Cybersecurity-07-12-2017/ [http://perma.cc/B6F8-6PQ4] ("The new enforcement co-directors' very clear initial statements on cybersecurity mean that firms should expect cybersecurity enforcement and examination activity to continue under the new administration.").

requirements.[51] Through these actions, a clearer picture of what the SEC safeguards rule requires is emerging.[52]

On September 22, 2015, the SEC brought and settled an action against R.T. Jones Capital Equities Management, Inc. after its web server was compromised, resulting in unauthorized access to the data therein.[53] The SEC asserted that R.T. Jones failed to comply with the written policy requirement because it did not address the security and confidentiality of its clients' personally identifiable information (PII) on the server or adequately address the protection of PII from "anticipated threats or unauthorized access."[54] The SEC noted that R.T. Jones did not schedule or conduct risk assessments regularly, or have a plan in place to respond to cybersecurity incidents.[55] The SEC also noted the absence of technical safeguards, such as a firewall or the use of encryption on the server containing PII.[56] This action marked a change from previous enforcement actions, as it "underscore[d] that investment advisers and broker-dealers may face regulatory scrutiny and enforcement actions even *without* a concrete, identifiable financial impact to clients."[57]

The SEC found it significant that R.T. Jones promptly undertook remedial efforts and cited those efforts in its decision.[58] The first set of remedial measures included oversight changes, such as drafting and implementing an information-security policy.[59] The second set involved technical changes, including ceasing to store PII on its webservers, encrypting PII stored on its

51. *See generally* Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78,021, Investment Advisers Act Release No. 4415 (June 8, 2016); Craig Scott Capital, LLC, Exchange Act Release No. 77,595 (Apr. 12, 2016); R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204 (Sept. 22, 2015).

52. Carmen Germaine, *SEC Poised to Turn Cybersecurity Focus into Enforcement*, LAW360 (July 7, 2017, 12:09 PM), https://www.law360.com/articles/937197/sec-poised-to-turn-cybersecurity-focus-into-enforcement [https://perma.cc/TE7E-MMUG]. *See generally* Julie Kadish, *SEC's Focus on Enforcing Data Security Safeguards Continues: Lessons Learned from Its $1M Fine of Morgan Stanley*, DYKEMA (June 15, 2016), https://www.dykema.com/resources-alerts-sec-focus-on-enforcing-data-security-safeguards-continues-lessons-learned-from-its-1m-fine-of-morgan-stanley_06-15-2016.html [https://perma.cc/6ARA-8LBA].

53. R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204, at 2–3 (Sept. 22, 2015).

54. *Id.* at 2.

55. *Id.* at 3.

56. *Id.*

57. Timothy C. Blank et al., *SEC Cybersecurity Examinations and Enforcement: What Broker-Dealers and Investment Advisers Need to Know*, DECHERT LLP (Sept. 29, 2015), https://s3.amazonaws.com/documents.lexology.com/729014f4-bfef-4c3c-96a5-4e4d64c01f22.pdf [https://perma.cc/FF5X-YN54]; *see also* Jenna N. Felz, *Data Security in the Financial Industry: Five Key Developments to Keep an Eye on in 2016*, DATA PRIVACY MONITOR (Jan. 27, 2016), https://www.dataprivacymonitor.com/financial-privacy/data-security-in-the-financial-industry-five-key-developments-to-keep-an-eye-on-in-2016/ [https://perma.cc/34JZ-429Y] ("Notably, there was no evidence of any harm to clients as a result of the hack.").

58. R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204, at 4 (Sept. 22, 2015).

59. *Id.*

internal networks, and installing tools to detect and respond to malicious activity.[60] The final change was the retention of a cybersecurity firm to provide reports and advice regarding the firm's security posture.[61]

The SEC elaborated on its requirements for an adequate safeguard policy in its action against Craig Scott Capital (CSC).[62] The action was not related to a breach but arose purely because CSC did not abide by the safeguards rule.[63] In this action, the SEC found CSC's written policy inadequate because it did not address how customer information would be handled internally.[64] The policy was also found inadequate because it was incomplete and insufficiently "tailored to the actual practices at CSC."[65]

In addition to the inadequacy of the written policies and procedures, the SEC noted that CSC did not even follow the written policy. The SEC also observed that CSC failed to encrypt customer information that was transmitted remotely despite including these measures in their written policy.[66]

In a subsequent action, the SEC addressed internal safeguards focused on employee access to confidential information. This action arose after a Morgan Stanley employee misappropriated customer data from approximately 730,000 accounts.[67] The confidential data was stored on the employee's personal server, which was likely hacked by a third party.[68] Some of the stolen data was then posted on a number of internet sites, with an offer of more stolen data for interested purchasers.[69]

The SEC stated that, despite having written policies and procedures, Morgan Stanley had breached the safeguards rule.[70] The safeguards were not reasonably designed to protect customers' PII because they did not "adequately address certain key administrative, technical and physical safeguards."[71] It found that Morgan Stanley failed to adequately restrict

60. *Id.*
61. *Id.* at 3–4.
62. Craig Scott Capital, LLC, Exchange Act Release No. 77,595, at 5 (Apr. 12, 2016).
63. *Id.*; Kadish, *supra* note 52 ("This settlement serves as a reminder that both firms and individuals can be fined and held accountable even if no customer is financially harmed.").
64. Craig Scott Capital, LLC, Exchange Act Release No. 77,595, at 5 (Apr. 12, 2016).
65. *Id.* at 2.
66. *Id.* at 6.
67. Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78,021, Investment Advisers Act Release No. 4415, at 2 (June 8, 2016); Press Release No. 15-334, U.S. Attorney's Office, S.D.N.Y., Former Morgan Stanley Financial Adviser Sentenced in Manhattan Federal Court for Illegally Accessing Confidential Client Information (Dec. 22, 2015), https://www.justice.gov/usao-sdny/pr/former-morgan-stanley-financial-adviser-sentenced-manhattan-federal-court-illegally-0 [https://perma.cc/LA3X-7RMR] ("MARSH illegally accessed the Bank's confidential client information in order to use it for his personal advantage as a private wealth management adviser at the Bank. From October 2013 through December 2014, MARSH was engaged in discussions regarding potential employment with two other financial institutions that are competitors of the Bank.").
68. Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78,021, Investment Advisers Act Release No. 4415, at 2 (June 8, 2016).
69. *Id.*
70. *Id.* at 5–6.
71. *Id.* at 6.

employee access to the data necessary to accomplish a legitimate business need.[72] Further, the SEC noted that Morgan Stanley did not monitor or analyze how employees were accessing data or using their system accesses.[73] For these reasons, the SEC found Morgan Stanley's policies to be inadequate.[74]

In addition to enforcement actions, the SEC releases guidance containing assessments and advice regarding cybersecurity that may indicate its expectations.[75] In preparing these assessments, the SEC performs examinations of covered entities and evaluates their policies, including assessing whether the policies were actually implemented.[76] They also evaluate how covered entities address areas including: "(1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response."[77] In performing the most recent assessment, the SEC found that while there were improvements in cybersecurity and safeguards from previous evaluations, the majority of policies and procedures still suffered from deficiencies.[78]

One issue that the SEC highlighted was the failure to reasonably tailor policies, such as through a lack of specificity.[79] The SEC also noted that some firms did not enforce their policies or had written policies that did not accurately reflect the actual practices that were employed.[80] The SEC went on to express concern that entities failed to perform ongoing system maintenance and omitted simple practices such as installing software patches addressing known vulnerabilities.[81] These concerns reflect several elements discussed above in the enforcement actions, including the failure to create a detailed, tailored plan and to implement technical operational safeguards.

The examples of robust security practices may constitute the most significant guidance. One recommendation was to perform "a complete inventory of data and information, along with classifications of the risks, vulnerabilities, data, [and] business consequences."[82] Complementing this recommendation, the SEC suggested that requests for access to data by employees should be tracked and that policies and procedures should address the modification of employee access rights when their need to access data changed.[83]

---

72. *Id.* at 2.
73. *Id.* at 4.
74. *Id.* at 6.
75. *See generally Observations from Cybersecurity Examinations*, RISK ALERT (U.S. Sec. & Exch. Comm'n, Aug. 7, 2017), https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf [https://perma.cc/N7LG-6VRK].
76. *Id.* at 1.
77. *Id.*
78. *Id.*
79. *Id.* at 3.
80. *Id.* at 4.
81. *Id.*
82. *Id.* at 4–5.
83. *Id.* at 5.

Another significant recommendation was to establish a plan of action that outlined what to do and who to contact in the event of a breach.[84] Beyond this, the SEC recommended that senior management be involved in vetting and approving the policies and procedures.[85]

The SEC also recommended utilizing vulnerability scans to identify weaknesses and adequately remediating any identified issues.[86] This recommendation reflects some of the enforcement actions the SEC took with regard to known issues that the covered entities failed to address. The SEC found it problematic that high-risk vulnerabilities discovered during such testing were not properly addressed.[87]

The SEC recommended that covered entities provide guidance to employees explaining how the networks and equipment should be appropriately accessed and used.[88] It suggested that entities consider including mandatory information-security training in their policy, as well as implementing procedures to ensure that such training was completed.[89] The SEC also expressed concern that some entities did not enforce mandatory training despite including it in their policies.[90]

2. They Want to Be a Part of It: New York, New York Department of Financial Services

In 2017, the NYDFS promulgated regulations regarding cybersecurity at financial services companies.[91] These regulations apply to entities that operate under a "certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law."[92] This has the potential to "encompass an extremely broad range of businesses given the vast scope of New York banking, insurance, and financial services laws."[93] Entities that are likely to be covered include, "commercial banks, foreign banks with New York State-licensed offices, mortgage brokers and servicers, small-loan lenders and money transmitters doing business in New York."[94] In addition, these entities are responsible for the actions of third parties they share data with.[95]

---

84. *Id.*
85. *Id.*
86. *Id.* at 4.
87. *Id.*
88. *Id.* at 5.
89. *Id.*
90. *Id.* at 4.
91. N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017).
92. *Id.* § 500.01.
93. Krimminger et al., *supra* note 18, at 2.
94. Adam J. Fleisher & Nathan D. Taylor, *New York Cybersecurity Regulations: What Do They Mean and When Do They Mean It By?*, MORRISON & FOERSTER LLP, at 1–2 (Mar. 23, 2017), https://media2.mofo.com/documents/170323-ny-cybersecurity-regulations.pdf [http://perma.cc/7LHA-MFL6].
95. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.

In contrast to the jurisdiction of the SEC, the NYDFS does not directly license or regulate investment advisors, brokers, or dealers in New York.[96] However, the entities that are regulated by the NYDFS are often affiliated with investment advisers, brokers, and dealers. Because of this, they usually share computer and communications infrastructure with entities regulated by the SEC, meaning that these entities are often subject to both regulations.[97] This is because it would be inefficient for many of those entities to deploy separate networks for different branches of business.[98] These factors are significant in evaluating the NYDFS regulations since they possibly reach beyond the entities they directly address.[99] For the purposes of this Note, it is enough to recognize that the NYDFS regulations will likely apply to some entities covered by the SEC regulations.

The NYDFS promulgated these regulations because they believed there was a need for minimum standards due to the serious nature of the risk.[100] The regulations require covered entities to assess the specific risks they face and adopt a program designed to protect themselves and their customers.[101]

The NYDFS requires that entities "implement and maintain a written policy or policies . . . setting forth [their] policies and procedures" to protect their information systems.[102] These policies must address concerns such as customer data privacy, incident response, and systems and network security.[103] The NYDFS regulations define functions that should be addressed, such as detecting cybersecurity events, responding to and mitigating events that occur, recovering from the event and restoring normal operations and services, and fulfilling reporting requirements.[104] The NYDFS regulations identify fourteen specific areas that should be addressed when applicable, including data governance and classification, asset

96. Marcus A. Asner et al., *New York Department of Financial Services Issues Final Cybersecurity Regulations*, ARNOLD & PORTER KAYE SCHOLER (Feb. 22, 2017), https://www.arnoldporter.com/en/perspectives/publications/2017/02/new-york-department-of-financial-services [https://perma.cc/KRT8-Q242].

97. *Id.* ("[T]he use of common computer and communications platforms among affiliated financial services firms may as a practical matter regulate the operations of broker-dealer and investment adviser firms that are affiliated with Covered Entities.").

98. Kilpatrick Townsend & Stockton LLP, *Cyber Winter Is Here, and Coming to Regulation: New York Cybersecurity Rule Ice Dragon Heading for the Wall*, JD SUPRA (Oct. 4, 2017), https://www.jdsupra.com/legalnews/new-york-cybersecurity-rule-ice-dragon-40435/ [https://perma.cc/LY8V-E4UY] ("Many large institutions gain efficiencies by deploying centrally managed information technology platforms and cybersecurity programs and tools. Thus, if only a part of an organization falls under the Cybersecurity Rules, it would be impractical for the larger enterprise not to adhere to the Cybersecurity Rules.").

99. Steven R. Chabinsky et al., *Cybersecurity: Regulators Show Their Teeth*, WHITE & CASE LLP (Sept. 20, 2017), https://www.whitecase.com/sites/whitecase/files/files/download/publications/cybersecurity-regulators-show-teeth-2.pdf [http://perma.cc/35N2-W5NC].

100. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.

101. *Id.*

102. *Id.* § 500.03.

103. *Id.*

104. *Id.* § 500.02.

inventory, access controls, and systems and network security and monitoring.[105]

Covered entities also must have incident response plans that address internal processes; goals; clearly defined "roles, responsibilities and levels of decision-making authority"; information sharing; methods of vulnerability identification and remediation; methods of documentation and reporting; and the evaluation and revision of such plans following a cybersecurity event.[106]

The NYDFS regulations also require that the compliance plan implement methods of testing and monitoring, which permits entities to choose between continuous monitoring or periodic penetration testing and vulnerability assessments.[107] The NYDFS does not mandate any specific method for continuous monitoring.[108] However, the monitoring should be designed to identify changes that potentially create vulnerabilities and activities that may be malicious.[109] The NYDFS explicitly provides that "periodic manual review of logs and firewall configurations" are not sufficient steps to satisfy the continuous monitoring obligation.[110]

With regard to personnel with access to systems, the NYDFS requires that covered entities implement access controls and periodically review what privileges employees require.[111] Entities must also implement systems to monitor user activity and detect unauthorized activity by those users.[112] They also require the entity to regularly provide current cybersecurity training.[113]

The NYDFS regulations require some specific measures that act as effective controls on data flows, such as multifactor authentication when the entity allows the internal network to be accessed externally through remote access or other means.[114] A second specified measure is implementing encryption to protect customer data both while traversing external networks and while at rest internally.[115]

105. *Id.* § 500.03 (listing "(a) information security; (b) data governance and classification; (c) asset inventory and device management; (d) access controls and identity management; (e) business continuity and disaster recovery planning and resources; (f) systems operations and availability concerns; (g) systems and network security; (h) systems and network monitoring; (i) systems and application development and quality assurance; (j) physical security and environmental controls; (k) customer data privacy; (l) vendor and Third Party Service Provider management; (m) risk assessment; and (n) incident response").

106. *Id.* § 500.16.

107. *Id.* § 500.05.

108. *Frequently Asked Questions Regarding 23 NYCRR Part 500*, N.Y. DEP'T FIN. SERVICES, http://www.dfs.ny.gov/about/cybersecurity_faqs.htm [https://perma.cc/48YP-A7H2] (last updated Aug. 9, 2018).

109. *Id.*

110. *Id.*

111. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.07.

112. *Id.* § 500.14.

113. *Id.*

114. *Id.* § 500.12.

115. *Id.* § 500.15(a).

3. The Final Countdown to the GDPR

On April 27, 2016, the EU adopted the GDPR.[116] The Regulation became effective on May 25, 2018.[117] The jurisdiction provided under the GDPR reaches further than either the SEC or NYDFS regulations. The GDPR applies

> to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to . . . the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or . . . the monitoring of their [behavior] as far as their [behavior] takes place within the Union.[118]

This broad territorial scope means that the physical location of the entity will be less significant, with the focus instead being on where the data came from.[119] Practically, this may mean that companies marketing goods or services in the EU will be subject to the GDPR.[120] This would include any financial institution marketing services to EU clients.

The Regulation states that to protect customer data, "measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected."[121] The GDPR also requires a written policy or procedure in the form of a data protection impact assessment (DPIA) whenever activities involve a high risk to the rights and freedoms of EU persons.[122] While the analysis necessary to evaluate high risk is not wholly settled, the EU Working Party 29 (WP29)[123] suggests a list of ten factors and recommends that if two are met a DPIA should be

116. Commission Regulation 2016/679, 2016 O.J. (L 119) 1, 88 (EU).

117. *Id.* art. 99.

118. *Id.* art. 3.

119. Jonathan Millard & Tyler Newby, *EU's General Data Protection Regulation: Sweeping Changes Coming to European and U.S. Companies*, A.B.A. (May 23, 2016), http://apps.americanbar.org/litigation/committees/technology/articles/spring2016-0516-eu-general-data-protection-regulation.html [https://perma.cc/K3UH-8Y78] ("Jurisdiction will . . . be measured digitally rather than physically, paying less attention to the physical location of the entity undertaking the processing.").

120. Courtney M. Bowman, *A Primer on the GDPR: What You Need to Know*, PROSKAUER (Dec. 23, 2015), http://privacylaw.proskauer.com/2015/12/articles/european-union/a-primer-on-the-gdpr-what-you-need-to-know/ [https://perma.cc/7JMX-W2RP].

121. Commission Regulation 2016/679, *supra* note 116, recital 83.

122. *Id.*

123. Skadden, Arps, Slate, Meagher & Flom LLP, *Privacy & Cybersecurity Update—October 2017*, JD SUPRA (Nov. 2, 2017), https://www.jdsupra.com/legalnews/privacy-cybersecurity-update-october-54232/ [https://perma.cc/P7SR-AY7K] ("WP29 is an EU advisory body made up of representatives from the data protection authorities of EU members. It is charged with providing expert guidance on data protection issues and promoting uniform application of data protection laws across the EU. Though not technically binding on EU member states' individual data protection commissioners, WP29's guidance carries a good deal of weight when the individual commissioners evaluate data privacy issues.").

performed.[124] Two factors the WP29 identifies that almost certainly apply to U.S. financial institutions are sensitive data, such as financial data, and data that will be transferred outside of the EU.[125] Of the remaining factors, several seem likely to apply to financial institutions as well.[126] While financial institutions will always need to perform a fact-specific analysis to evaluate whether a DPIA is necessary, the WP29 guidance suggests that it will nearly always be necessary in this context.[127]

While a DPIA evaluates more than security, one of only four requirements of such an assessment is to identify the measures an entity intends to take to mitigate the risks to personal data,[128] which indicates the significance of this element.[129] The measures adopted should be based on factors such as costs, state of the art, risk, and severity of the rights at issue, and they also must address issues such as data flow, unauthorized access, and destruction or degradation of data, among a number of other concerns.[130]

The GDPR also suggests the use of some specific measures such as encryption, de-identification, security-measure testing, and the remediation of any vulnerabilities uncovered as a result of such testing.[131] It specifically suggests that pseudonymization and encryption might be appropriate measures to adopt.[132] The GDPR also recommends establishing means to regularly test and evaluate the effectiveness of the adopted measures.[133]

A covered entity may be able to avoid the notification requirements in the GDPR if the breach "is unlikely to result in a risk to the rights and freedoms of natural persons."[134] For example, if a covered entity utilizes encryption to make the information unintelligible, they may not have to report the breach.[135] It is important to recognize that this requires reevaluations and can change with time, as vulnerabilities can be discovered and encryption

124. Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679*, at 7–9, WP 248 (Apr. 4, 2017).

125. *Id.* at 8–9.

126. *See id.* at 7–10.

127. *See id.* at 9–10.

128. Commission Regulation 2016/679, *supra* note 116, art. 35.

129. *Id.*

130. *Id.* art. 32.

131. Julie Brill, Comm'r, Fed. Trade Comm'n, Remarks, Two-Way Street: U.S.-EU Parallels Under the General Data Protection Regulation Ghostery/Hogan Lovells Data Privacy Day (Jan. 21, 2016), https://www.ftc.gov/system/files/documents/public_statements/910663/160121hoganghostery_dpd.pdf [https://perma.cc/2GAS-2PEU].

132. Commission Regulation 2016/679, *supra* note 116, art. 32.

133. *Id.*

134. *Id.* art. 33.

135. Article 29 Data Protection Working Party, *Guidelines on Personal Data Breach Notification Under Regulation 2016/679*, at 9, WP 250 (Oct. 3, 2017).

keys can be compromised.[136] In evaluating that risk, the covered entity should objectively consider "both the likelihood and severity of the risk."[137]

The WP29 interprets elements of the GDPR to create an obligation to "have internal processes in place to be able to detect and address a breach."[138] This could include technical measures that allow the entity "to define events and alerts."[139] The WP29 recommends that the measures adopted be included in the entities' incident response plan.[140]

B. The Costs of Regulation

Regulations inevitably create costs, which have real effects on economies, consumers, and institutions.[141] The total estimated cost of regulatory compliance in the United States in 2008 was $1.75 trillion.[142] There are substantial benefits to regulation that can offset these costs, and regulation is a necessary element in a functioning country and society.[143] However, regulation clearly creates substantial burdens as well.[144] These burdens are shared between public and private institutions, and between businesses and their customers.[145] When compliance costs go up, some portion is pushed onto consumers or employees.[146]

---

136. *Id.* at 16 ("A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the [covered entity] and its staff. Provided the encryption key remains within the secure possession of the [covered entity] and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.").

137. *Id.* at 20. Factors to consider include: (1) "the type of breach"; (2) "the nature, sensitivity, and volume of personal data"; (3) "ease of identification of individuals"; (4) "severity of consequences for individuals"; (5) "special characteristics of the individual"; (6) "the number of affected individuals"; and (7) "special characteristics of the data controller." *Id.* at 20–22.

138. *Id.* at 10.

139. *Id.*

140. *Id.*

141. *See* JOHN BACE ET AL., UNDERSTANDING THE COSTS OF COMPLIANCE 4–5 (2006), http://logic.stanford.edu/POEM/externalpapers/understanding_the_costs_of_c_138098.pdf [https://perma.cc/47UX-QRCH]; Kevin Dobbs, *Since Dodd-Frank, Compliance Costs Up at Least 20% for Many U.S. Banks*, S&P GLOBAL MKT. INTELLIGENCE (Oct. 19, 2017, 9:53 AM), https://marketintelligence.spglobal.com/our-thinking/ideas/since-dodd-frank-compliance-costs-up-at-least-20-for-many-u-s-banks; William Dunkelberg, *The Insidious Cost of Regulation*, FORBES (Apr. 4, 2017, 10:45 AM), https://www.forbes.com/sites/williamdunkelberg/2017/04/04/the-insidious-cost-of-regulation/#68798dc35c7b [https://perma.cc/WC2K-Z87T].

142. NICOLE V. CRAIN & W. MARK CRAIN, THE IMPACT OF REGULATORY COSTS ON SMALL FIRMS 6 (2010), https://www.sba.gov/sites/default/files/The%20Impact%20of%20Regulatory%20Costs%20on%20Small%20Firms%20(Full)_0.pdf [https://perma.cc/654C-39T3].

143. *Id.* at 10–11.

144. *Id.* at 6.

145. *Id.*

146. *See* Dobbs, *supra* note 141. *See generally* CRAIN & CRAIN, *supra* note 142.

Another result of rising compliance costs is consolidation. Some predict that compliance will drive small institutions out of the marketplace.[147] Compliance costs more for smaller businesses than it does for larger ones, with the costs of compliance estimated at $10,585 per employee at a firm with fewer than twenty employees, compared to $7755 per employee at a firm with 500 employees or more.[148] This means that smaller firms pay around 36 percent more per employee than larger firms do, largely because many compliance regimes have fixed costs that are diluted with scale.[149]

As profit margins decline and compliance costs increase, the number of small financial institutions has dwindled.[150] This could result in less competition and decreased consumer choice, barriers to new entrants who could offer improved services, and fewer institutions willing to underwrite smaller businesses.[151]

While cybersecurity regulations are necessary, unnecessary costs should be mitigated. This Note recommends that regulators identify the areas where a single process or action could satisfy the different regulatory regimes and provide collaborative guidance in those areas. Part II explores some of these areas of overlap.

II. IDENTIFYING AREAS OF OPPORTUNITY FOR COORDINATION

These regulations, where they address cybersecurity posture and plans, all attempt to accommodate changing cybersecurity needs. The three regulatory schemes presented above are representative of cybersecurity regulations governing financial institutions but are not exhaustive. Since financial

147. Dobbs, *supra* note 141 ("[S]ome in the industry expect M&A to continue for years and eventually result in a banking landscape all but devoid of small institutions.").

148. CRAIN & CRAIN, *supra* note 142, at 8.

149. *Id.*; Hester Peirce, *Dwindling Numbers in the Financial Industry*, BROOKINGS (May 15, 2017), https://www.brookings.edu/research/dwindling-numbers-in-the-financial-industry/ [https://perma.cc/7YQ3-5EMP] ("Many regulations disproportionately burden small [financial institutions] that are not subsidiaries of a larger firm with extensive compliance resources.").

150. Peirce, *supra* note 149 ("The number of [broker-dealers] has declined fairly consistently over the last decade. In March 2017, there were 3,989 [broker-dealers] registered with the SEC compared to 5,892 in March 2007, a more than thirty percent drop."); *see also* Nick Fera, *How Small Broker-Dealers Can Survive in Today's Shifting Trading Landscape*, THESTREET (Sept. 10, 2015, 10:25 AM), https://www.thestreet.com/story/13267934/1/are-you-a-small-broker-dealer-here-s-how-you-can-survive.html [http://perma.cc/E7BZ-D68A] ("The number of broker-dealer firms registered with the Financial Industry Regulatory Authority dropped to 4,040 by April 2015 from 4,578 in 2010, a nearly 12% decrease . . . . Most analysts and industry experts agree that there are two primary factors fueling this trend: shrinking margins and swelling compliance costs."); Bruce Kelly, *With Margins Crashing, Broker-Dealers Look to Merge: Report*, INVESTMENTNEWS (Sept. 21, 2017, 2:15 PM), http://www.investmentnews.com/article/20170921/FREE/170929982/with-margins-crashing-broker-dealers-look-to-merge-report [https://perma.cc/34KR-ZTDT] ("The number of [Independent Broker-Dealers] has declined 28%, with 904 open for business in 2015, compared to 1,255 such firms that were up and running in 2005. And with increased regulation pressuring profits, broker-dealer operating margins dropped from 12% in 2006 to just 3% in 2016.").

151. Peirce, *supra* note 149.

institutions fall under the jurisdiction of each of these bodies, as well as others, it would be valuable to ascertain where requirements are common and can be adopted as part of a single compliance plan.

Part II focuses on identifying elements common to all three regulatory regimes. The purpose is to recognize the areas where the regulatory bodies are operating in the same or similar spaces. Part II is not intended to be a comprehensive analysis of every area where harmonization could occur. Rather, it identifies a few requirements that are costly to implement and significant within the regulatory regimes to serve as examples. Part II.A addresses data classification, II.B the formulation of written policies, and II.C the implementation of encryption.

A. Classing Up the Joint: Data Classification

Data classification "is the process of identifying, understanding and mapping out the data flows of an organisation."[152] This requires an exhaustive cataloging of the information held by the entity, with the end product being a visual representation of data assets and flows.[153] This visualization illustrates the different types of data held by the organization and the way that data is transferred and disclosed both within the organization and to third parties.[154] Engaging in such a process can provide an entity with a comprehensive understanding of how their data travels both inside and outside of their networks.[155] Although this area is discussed the most obliquely by all three regulatory regimes, it is fundamental to a discussion of compliance under any of them.[156] As a practical matter, data classification is necessary to comply with all three regulatory regimes.[157]

In its action against Morgan Stanley, the SEC suggests an obligation to limit employee access based on need.[158] This indicates an expectation that covered entities evaluate employee needs for data and provide the lowest level of access privilege necessary to satisfy those needs. This is significant because it requires that an entity classify the data it holds and contemplate what controls it should exercise over the movement of that data.

The SEC also indicated the necessity of data classification through guidance and suggested that entities have "a complete inventory of data and information, along with classifications of the risks, vulnerabilities, data, [and] business consequences."[159] The SEC also recommends tracking

152. BAKER & MCKENZIE LLP, EU GENERAL DATA PROTECTION REGULATION IN 13 GAME CHANGERS 33 (2018), https://www.bakermckenzie.com/en/-/media/files/insight/publications/2018/05/bk_uk_eugeneraldataprotection_mar2018.pdf.

153. *Id.*

154. *Id.*

155. *Id.*

156. *Id.* at 34 ("Understanding one's . . . data flows . . . is an essential prerequisite for any privacy compliance strategy.").

157. *Id.*

158. Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78,021, Investment Advisers Act Release No. 4415, at 2 (June 8, 2016).

159. *Observations from Cybersecurity Examinations*, *supra* note 75, at 4–5.

employee access requests and creating policies and procedures governing the modification of access rights.[160] These recommendations indicate that entities should catalog the data they hold, consider the categories of data in terms of risk, implement safeguards based on those considerations, and limit and monitor access to the data.

Finally, it is significant to note that the SEC requires a written policy that is reasonably tailored. This requires "more than a generic, cookie-cutter cybersecurity policy."[161] To formulate such a policy, covered entities must meaningfully analyze the specific risks they face.[162] The SEC guidance notes that narrowly scoped and vague policies do not satisfy the reasonably tailored requirement, nor do policies that only offer general guidance or limited examples of safeguards.[163] For a policy to be reasonably tailored, it is crucial to identify how data and communications travel within the organization and to prioritize data resources "based on their classification, criticality, and business value."[164] By approaching the process in this way, entities will be able to identify what requires protection and the appropriate level of protection, which will lead to a reasonably tailored policy.[165]

The NYDFS regulations require that a covered entity assess data governance and classification, asset inventory and device management, and access controls and identity management.[166] Covered entities must identify what material nonpublic information they hold and where they are holding that information, as such cataloging "is foundational for compliance with the Cybersecurity Rules."[167]

Many of the requirements under the NYDFS regulations can only be achieved after the data the covered entity holds has been classified. For example, covered entities must implement user access controls that limit personnel access to personal information.[168] This requires covered entities to identify the information and systems that individual employees need access to and to only permit the level of access that is required.[169] A covered entity will need to identify all the relevant data in order to satisfy this

160. *Id.*
161. Blank et al., *supra* note 57.
162. *See id.*
163. *Observations from Cybersecurity Examinations*, *supra* note 75, at 3.
164. NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY app. A, tbl.2 (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [https://perma.cc/KDT3-YHRZ].
165. *Id.* at 8 ("Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts.").
166. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.03 (2017).
167. Kilpatrick Townsend & Stockton LLP, *supra* note 98.
168. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.07.
169. Joseph Vitale et al., *NYDFS Proposed Cybersecurity Regulation for Financial Services Companies*, SCHULTE ROTH & ZABEL LLP, at 4 (Sept. 15, 2016), https://www.srz.com/images/content/1/4/v2/145023/091516-NYDFS-Proposes-Detailed-and-Sweeping-Cybersecurity-Regula.pdf [http://perma.cc/8UQG-Q3X5].

requirement.[170] Similarly, the covered entities must assess all data and systems in order to identify which will be governed by the specified measures discussed above, such as multifactor authentication and encryption requirements, and take steps to satisfy the requirements.[171]

The GDPR includes an accountability principle, which obligates covered entities to maintain records that demonstrate their compliance with the GDPR.[172] This includes recording the purpose for which they hold data as well as the ways they are processing it.[173] The covered entity must also track where the data is transferred, including locations outside the EU, and how that data is handled, including how long it is retained.[174] Finally, it must document the technical and organizational measures taken to demonstrate compliance with the requirements.[175] To satisfy this obligation, the United Kingdom Information Commissioner's Office recommends that covered entities "document what personal data [they] hold, where it came from and who [they] share it with" and adds that it may be necessary "to [organize] an information audit."[176]

In addition to facilitating compliance with the accountability requirements, data classification would permit timely compliance with other obligations, such as providing requested data to supervisory authorities.[177] It would also allow covered entities to demonstrate that their plans protect data by design and by default, as required.[178] A final benefit would be an enhanced ability to assess the risks to the rights and freedoms of EU citizens. Since the GDPR advocates such a risk-based approach, data classification will help an entity determine the extent of their GDPR obligations.[179]

---

170. PWC Fin. Crimes Unit, *Cyber: New York Regulator Moves the Goalposts*, FIN. CRIMES OBSERVER (Sept. 2016), https://www.pwc.com/us/en/financial-services/financial-crimes/publications/assets/NY-DFS-proposes-cybersecurity-regulations.pdf [https://perma.cc/8KS3-SBQV].

171. Asner et al., *supra* note 96.

172. Commission Regulation 2016/679, *supra* note 116, art. 30; *Preparing for the General Data Protection Regulation (GDPR): 12 Steps to Take Now*, INFO. COMMISSIONER'S OFF. 3 (2018) [hereinafter *Preparing for the GDPR*], https://web.archive.org/web/20180706184647/https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

173. Hanno Timner & Alex van der Wolk, *M&A and the New European Data Protection Rules: Additional Risks for Transactions and How to Avoid Them*, 20 WALL STREET LAW., July 2016, at 6.

174. *Id.*

175. *Id.*

176. *Preparing for the GDPR*, *supra* note 172, at 3.

177. BAKER & MCKENZIE LLP, *supra* note 152, at 35.

178. *Id.*; Teresa Troester-Falk & Paul Breitbarth, *Does GDPR Article 30 Require a Data Inventory?*, NYMITY (July 2017), https://www.nymity.com/~/media/NymityAura/Resources/Nymity%20Insights/Nymity_Insights-GDPR_Article_30_Data_Inventory.pdf [https://perma.cc/8WSP-SW27] ("Logically, until an organisation truly understands what personal data they have, where it is located, and how it moves through and out of the organisation, it is not possible to protect it nor is it possible to fully comply with the GDPR (at least in spirit).").

179. BAKER & MCKENZIE LLP, *supra* note 152, at 34.

B. Words Are Easy, Like the Wind; but Writing Is Hard

All three regulatory regimes require a documented policy, with some differences in explicitness and the factors that must be considered. In cybersecurity examinations, the SEC focused on "(1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response."[180] The SEC's focus on these six factors indicates that these factors influence whether the policy is reasonably designed to protect consumer information and is tailored to the entity's needs. A covered entity should closely consider these factors in formulating its written policy.

Early SEC enforcement actions provide insight into what it expects the written policy to contain, such as technical security measures and administrative procedures for addressing security issues.[181] The SEC actions indicate that the policies must be tailored and, therefore, specific.[182] The SEC also found a written policy insufficient because it failed to provide guidance and training regarding data protection to personnel.[183]

Subsequent enforcement actions indicate more specific requirements and note their subjects' failure to address elements such as periodic risk assessments, firewall use, a response plan in the event of a breach, or measures for handling data.[184] This marks a change from the early enforcement actions, as the SEC looks beyond a failure to address known issues or implement the most basic of security measures. These actions suggest that the SEC will take a closer look at the policies and evaluate the measures taken on a more technical level moving forward. A part of this more technical analysis seems to include assessing whether the policy reflects a real consideration of the unique infrastructure utilized by a covered entity in deciding whether it was appropriately tailored.[185] A final development appears to be a requirement to include procedures to implement and monitor employee access controls.[186]

The NYDFS regulations also require that the written policy address physical, administrative, and technical controls.[187] The written policy must comprehensively outline all aspects of the entity's cybersecurity program and identify how the entity complies with each element of the regulations.[188] Although more explicit and extensive than the requirements the SEC has articulated, the NYDFS regulations include many similar elements. Specific

180. *Observations from Cybersecurity Examinations*, *supra* note 75.

181. *See generally* Marc A. Ellis, Exchange Act Release No. 64,220 (Apr. 7, 2011); Commonwealth Equity Servs., LLP, Exchange Act Release No. 60,733, Investment Advisers Act Release No. 2929 (Sept. 29, 2009).

182. *See* Marc A. Ellis, Exchange Act Release No. 64,220, at 3 (Apr. 7, 2011).

183. *Id.*

184. *See* R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204, at 3 (Sept. 22, 2015).

185. *See* Craig Scott Capital, LLC, Exchange Act Release No. 77,595, at 2 (Apr. 12, 2016).

186. *See* Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78,021, Investment Advisers Act Release No. 4415, at 2–3 (June 8, 2016).

187. Chabinsky et al., *supra* note 99.

188. Vitale et al., *supra* note 169, at 3.

elements include measures addressing information security, data governance and classification, asset inventory and device management, access controls and identity management,[189] systems and network security, systems and network monitoring, customer data privacy, and incident response.[190] The plan must also address the cybersecurity training program.[191]

It is also likely that financial institutions will be required to perform a DPIA under the GDPR.[192] This assessment must include a list of the actions the entity will take and the tools they will employ to protect their data.[193] Even absent a DPIA, the GDPR requires a policy that includes "appropriate technical and organisational measures."[194] This means that the policies must address security risks as they affect the "confidentiality, integrity, availability and resilience" of systems, the entity's ability to maintain "availability and access to personal data," and the "testing, assessing and evaluating" of measures in place.[195] These measures should be based on the available technology as well as context, costs, and risks.[196]

The WP29 also indicates that measures should be in place to manage the network through traffic analysis.[197] It identifies the development of capabilities aimed at preventing a breach when possible, and reacting in a timely manner when not, as key to a data security policy.[198] Finally, it identifies the detection, remediation, and timely reporting of a breach as essential elements of a security policy.[199]

C. 5 14 3 18 25 16 20 9 15 14

Encryption is the "process of changing plaintext into ciphertext for the purpose of security or privacy."[200] Plaintext is what you are reading now, text that has not been coded or encrypted to make it unintelligible.[201] Somewhat circuitously, ciphertext is text that has been encrypted or rendered unintelligible through the use of a cipher.[202] Plaintext is transformed into

189. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.14 (2017) (including specific "policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users").

190. *Id.* § 500.03.

191. *Id.* § 500.14.

192. *See supra* Part I.A.

193. Commission Regulation 2016/679, *supra* note 116, art. 35.

194. *Id.* art. 32.

195. *Id.*

196. *Id.*

197. Article 29 Data Protection Working Party, *supra* note 135, at 10.

198. *Id.* at 6.

199. *Id.* at 11.

200. ELAINE BARKER, NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUBLICATION 800-175B, GUIDELINE FOR USING CRYPTOGRAPHIC STANDARDS IN THE FEDERAL GOVERNMENT: CRYPTOGRAPHIC MECHANISMS 5 (2016), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf [https://perma.cc/L3WB-Q3L5].

201. *Id.* at 7.

202. *Id.* at 4.

ciphertext through the use of cryptographic methods.[203] These methods rely on the use of an algorithm[204] and a key.[205] These components are used in conjunction to encrypt and decrypt the data.[206] Since the algorithm is usually publicly available, the secrecy of the key is what provides the security benefits derived from the use of cryptography.[207] Two common types of cryptographic algorithms that permit relatively rapid data movement are cryptographic hash functions[208] and symmetric-key algorithms.[209]

Cryptographic algorithms have a finite lifetime, as they can be attacked and compromised over time, which prevents the algorithm from providing the desired level of protection.[210] This lifetime is often linked to the algorithm strength, which is measured by the difficulty of breaking the algorithm.[211] Algorithm strength can generally be increased by lengthening the key.[212] It is also critically important to adopt adequate safeguards for selecting and handling the keys themselves.[213]

The SEC has not created any rule-based requirement regarding the use of encryption.[214] Rather, it has suggested the need for encryption through

---

203. *Id.* at 1 ("Cryptography is a branch of mathematics that is based on the transformation of data and can be used to provide several security services . . . .").

204. *Id.* at 4 (defining cryptographic algorithm as "[a] well-defined computational procedure that takes variable inputs, including a cryptographic key (if applicable), and produces an output").

205. *Id.* (defining cryptographic key as "[a] parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot").

206. *Id.*

207. *Id.*

208. *Id.* at 19 ("A hash function (also called a hash algorithm) is a cryptographic primitive algorithm that produces a condensed representation of its input (e.g., a message). A hash function takes an input of arbitrary length and outputs a value with a predetermined length.").

209. *Id.* at 20 ("Symmetric-key algorithms (sometimes called secret-key algorithms) use a single key to both apply cryptographic protection and to remove or check the protection. For example, the key used to encrypt data (i.e., apply protection) is also used to decrypt the encrypted data (i.e., remove the protection) . . . .").

210. *Id.* at 27 ("The attack could be on the algorithm itself, or could be on the algorithm with a specific key length. In the latter case, the use of a longer key may prevent a successful attack, or at least delay it for a period of time.").

211. *Id.* at 26 ("Breaking a cryptographic algorithm can be defined as defeating some aspect of the protection that the algorithm is intended to provide. For example, a block cipher encryption algorithm that is used to protect the confidentiality of data is broken if, with an acceptable amount of work, it is possible to determine the value of its key or to recover the plaintext from the ciphertext without knowledge of the key.").

212. *Id.* at 27 ("The approved security strengths for federal applications are 112, 128, 192 and 256 bits. Note that a security strength of 80 bits was previously approved as well." (emphasis omitted)).

213. *Id.* at 37 ("[T]he security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys themselves.").

214. NEXT Fin. Grp., Inc., Initial Decision Release No. 349, at 40 (Sec. & Exch. Comm'n ALJ June 18, 2008) ("The SEC neither established minimum standards nor discussed encryption when it proposed and adopted Regulation S-P.").

enforcement actions[215] and guidance.[216] The SEC noted in its action against R.T. Jones that a failure to encrypt client PII was problematic.[217] While enumerating positive changes made by R.T. Jones, the SEC specifically mentioned that the company began encrypting client PII.[218] In the CSC enforcement action, the SEC also discussed the failure to use encryption.[219] The attention to encryption in two of its most recent enforcement actions likely indicates that the SEC views encryption as an important measure to consider.

The SEC guidance also focused on encryption and described it as a potential part of a robust security policy.[220] The encryption recommendation is significant since it indicates that the SEC expects a network to be adequately designed to limit the damage caused by an intrusion. The encryption recommendation indicates that the SEC recognizes this as a useful tool in mitigating damage and in rendering information on a network inaccessible in the event of a breach.

The NYDFS regulations require that data both in transit and at rest be encrypted unless the entity's chief information security officer finds that it is infeasible.[221] While requiring that data "in transit over external networks and at rest" be encrypted, the NYDFS offers little guidance regarding how it should be implemented beyond that it must be based on a risk assessment.[222] Notably missing is guidance—like that issued by New York State to state agencies—regarding acceptable forms of encryption, including minimum bit strength and minimum key length.[223]

The GDPR recommends encryption as a possible measure for entities to adopt.[224] It also permits covered entities to avoid breach disclosure if the information breached is not intelligible due to appropriate technical

---

215. Craig Scott Capital, LLC, Exchange Act Release No. 77,595, at 5–6 (Apr. 12, 2016); R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204, at 3 (Sept. 22, 2015).

216. *Observations from Cybersecurity Examinations*, *supra* note 75, at 5.

217. R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204, at 3 (Sept. 22, 2015).

218. *Id.*

219. Craig Scott Capital, LLC, Exchange Act Release No. 77,595, at 6 (Apr. 12, 2016).

220. *Observations from Cybersecurity Examinations*, *supra* note 75, at 5.

221. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.15 (2017).

222. *Id.*

223. NYS OFFICE OF INFO. TECH. SERVS., NO: NYS-S14-007, IT STANDARD: ENCRYPTION (July 11, 2017), https://its.ny.gov/sites/default/files/documents/nys-s14-007_encryption_standard_2.pdf [https://perma.cc/6UPB-3CPL] ("Encryption products for confidentiality of data at rest and data in transit must incorporate Federal Information Processing Standard (FIPS) approved algorithms for data encryption at a minimum of 128 bit strength. Minimum key length for digital signatures and public key encryption is 2048. Hashing functions must have a minimum key length of 256.").

224. *GDPR Preparedness: An Indicator of Cyber Risk Management*, MARSH & MCLENNAN COMPANIES, at 6 (Oct. 2017), https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Cyber-Survey-Report-2017.pdf [https://perma.cc/V9MK-JXCF] ("Of the information security activities we asked about, only one—encrypting organizational computers—is explicitly encouraged by GDPR.").

measures, including encryption.[225] The WP29 endorses the use of a "state of the art algorithm."[226] It also states that the data should be properly encrypted.[227] The WP29 suggests that determining the proper encryption method requires an in-depth analysis of the risks the entity faces and the quality of the encryption method, including the level of protection it provides and the steps necessary to properly implement it.[228]

III. THE BENEFITS OF COORDINATION AND ITS APPLICATION IN CYBERSECURITY REGULATION

Part III proceeds in two parts. Part III.A discusses why collaboration is generally desirable and presents a few examples of mechanisms that could be used to effectuate international and domestic regulatory compromise. Part III.B explores how these mechanisms could be applied to further clarify the requirements for data classification, written policies, and encryption, and the specific benefits of such mechanisms.

A. The Why and How of Coordinating Cybersecurity Regulations

Cooperation between the regulatory bodies "will inevitably yield better, and more consistent, policy formation and guidance on both sides of the Atlantic."[229] This result will follow in part from the development of a common lexicon which can be leveraged in assessing the policies developed by covered entities.[230] Formalizing collaboration would support better policy by adding structure and sustainability to the process. This would promote shared learning as all three bodies apply cybersecurity principles in new contexts.[231] Such an arrangement could "improve communication/collective thinking and avoid missed opportunities to develop and coordinate . . . new policies."[232] Further, collaboration contributes to identifying and promoting baseline protections within the financial sector.[233] Cooperation in this area could contribute to improved cybersecurity and resiliency for the entire financial infrastructure.[234]

Collaboration will create benefits by limiting the degree of divergence between legal regimes.[235] Failing to align the requirements where possible results in unnecessary additional work streams that achieve compliance, but

225. Commission Regulation 2016/679, *supra* note 116, art. 34.
226. Article 29 Data Protection Working Party, *supra* note 135, at 15.
227. *Id.* at 16.
228. *Id.*
229. *See* PRIVACY BRIDGES, *supra* note 21, at 23.
230. *See* 2017 FIN. STABILITY OVERSIGHT COUNCIL ANN. REP. 7.
231. *See* PRIVACY BRIDGES, *supra* note 21, at 39.
232. *Id.* at 40.
233. 2017 FIN. STABILITY OVERSIGHT COUNCIL ANN. REP. 8–9, 130.
234. Grp. of 7 [G7], *Fundamental Elements of Cybersecurity for the Financial Sector* (2016), https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf [https://perma.cc/844L-2W42].
235. PRIVACY BRIDGES, *supra* note 21, at 23 ("To the extent that collaboration encourages consistency in guidance across the Atlantic, regulated parties can avoid the costs of having to comply with divergent legal regimes.").

little else.[236] Collaborating would minimize these unnecessary work streams and curb the additional compliance costs for companies operating in all three jurisdictions.[237] This would be especially beneficial for smaller entities that are already struggling with thinner margins, and it would potentially allow them to remain independent.[238] While it may seem like collaboration would only reduce these costs incrementally, it is important to remember the magnitude of foreign investment between the United States and the EU, which totaled $4.2 trillion in 2014.[239] The large amount of investment and close economic relationship between the United States and the EU would magnify even incremental cost reductions.

Despite differences in the way data protection is approached in the United States and the EU,[240] similarities in values and goals "provide[] common ground on which to build practical solutions."[241] The SEC, NYDFS, and EU all engage in various forms of international cooperation in the interest of furthering their regulatory goals.[242] A number of collaborative tools could be utilized by the three bodies to harmonize their regulatory schemes in areas where common goals are shared.[243] These include dialogues,[244] memoranda

236. *See* SIFMA Comment Letter, *supra* note 19, at 4.

237. *See* European Commission Memorandum MEMO/06/477, *supra* note 24, at 2, 7–8.

238. *See generally supra* Part I.B.

239. EUROPEAN UNION DELEGATION TO THE U.S., THE EUROPEAN UNION: A GUIDE FOR AMERICANS 16 (Sept. 20, 2014), https://eeas.europa.eu/sites/eeas/files/guide-for-americans_euintheus.pdf [https://perma.cc/ML87-VF29].

240. PRIVACY BRIDGES, *supra* note 21, at 23 ("Of course, each entity must remain free to reach whatever conclusions it believes are warranted under applicable EU and US law, respectively.").

241. *See id.* at 20 ("The possibility of . . . bridges derives from the common heritage of the EU and the US, the history of dialogue between them, and the common challenges they face. Despite their differences, the EU and US are both liberal democracies with a high degree of respect for the rule of law.").

242. *See generally* Letter from Isabelle Falque-Pierrotin, Chairwoman, Article 29 Working Party, to David Wright, Sec'y Gen., Int'l Org. of Sec. Comm'ns (Sept. 24, 2015), http://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150924__letter_of_the_art_29_wp_iosco.pdf [https://perma.cc/2GHW-KLFB]; Press Release No. 2013-131, Sec. & Exch. Comm'n, European Regulators Establish Supervisory Cooperation Arrangements Related to the Asset Management Industry (July 19, 2013), https://www.sec.gov/news/press-release/2013-131 [https://perma.cc/3PBD-UY7K]; N.Y. Dep't of Fin. Servs., *Interagency Agreements, Memoranda of Understanding and Other Information-Sharing Agreements*, N.Y. ST., http://www.dfs.ny.gov/legal/interagency_agree_mou.htm [http://perma.cc/TV3A-29HR] (last visited Aug. 24, 2018).

243. Mary Jo White, Chair, Sec. & Exch. Comm'n, Keynote Remarks at the International Bar Association Annual Conference Legal Practice Division Luncheon: Securities Regulation in the Interconnected, Global Marketplace (Sept. 21, 2016), https://www.sec.gov/news/speech/securities-regulation-in-the-interconnected-global-marketplace.html [http://perma.cc/YLJ6-5RQ7] ("Neither the SEC, nor other regulators, can go it alone, and we have many avenues to facilitate working together.").

244. *SEC Dialogues with Foreign Regulatory Authorities*, SEC. & EXCHANGE COMMISSION, https://www.sec.gov/about/offices/oia/oia_bilateraldialogs.shtml [http://perma.cc/J2XM-FS7B] (last visited Aug. 24, 2018); *see also* PRIVACY BRIDGES, *supra* note 21, at 38 ("[P]ropos[ing] that . . . European and US executive agencies and decision-making bodies engage in active dialogue and, where appropriate, effective coordination of their regulatory activity.").

of understanding,[245] nonbinding policy agreements,[246] and endorsing nonbinding technical standards.[247]

B. Applying the Benefits and Mechanisms to Requirements

This Part focuses on the benefits particular to the common requirements specified in Part II. It also explores how collaborative tools could be used to harmonize these areas. The purpose is to show how collaboration could operate, and the concrete benefits that such collaboration would create.

1. Breaking Down Data-Classification Barriers

Data classification is a critical first step underlying many of the requirements or expectations enunciated by all three bodies.[248] Performing that step provides a better understanding of what risks companies face based on their industry and infrastructure.[249] However, performing such an inventory can be complicated, complex, and resource intensive.[250] Given the need to perform some type of data-classification analysis to comply with all three regulatory regimes and the inevitable expense of doing so, cooperation between the three bodies to provide additional guidance in this area would be valuable.

In the United States, the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (the "NIST Framework") is a useful tool that provides guidance on how this step could be carried out. The NIST Framework recommends the performance of core functions, one of which is to "Identify."[251] This function requires the identification of a number of factors that are divided into categories that are relevant to assessing an organization's posture and risks.[252] Two

245. PRIVACY BRIDGES, *supra* note 21, at 5 (proposing that ties should be strengthened through "institutionaliz[ing] the working relationship between the Article 29 WP and the FTC" via a memorandum of understanding, and that this recommendation could be modified to apply to the SEC, NYDFS, and WP29).

246. Christopher Kuner, *An International Legal Framework for Data Protection: Issues and Prospects*, 25 COMPUTER L. & SECURITY REV. 307, 307–17 (2009) ("Various groups have issued policy documents containing voluntary data protection principles that are designed to be used on a global basis.").

247. *Id.* at 20 ("Several groups have already created technical standards for data protection and privacy which are not legally binding, but which can be adopted by States and organizations on a voluntary basis.").

248. *See generally supra* Part II.

249. NAT'L INST. OF STANDARDS & TECH., *supra* note 164; Troester-Falk & Breitbarth, *supra* note 178 ("Privacy officers are often taught that the first step in establishing a privacy program is to create a personal data inventory as way of prioritizing efforts, resources, assessing risks, and preparing for privacy incidents and breaches.").

250. Troester-Falk & Breitbarth, *supra* note 178 (proposing an interesting alternative to a traditional data inventory in the form of a data-processing inventory focused on the details of the processing activity).

251. NAT'L INST. OF STANDARDS & TECH., *supra* note 164, at 4.

252. *Id.* app. A, tbl.2 ("Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.").

subcategories are relevant to performing a data classification.[253] The first is mapping the organization and data flows and the second is prioritizing resources, including data, based on their "classification, criticality, and business value."[254] The NIST Framework does not mandate a specific methodology for carrying this task out and instead provides informative references.[255] These references are from a variety of organizations that offer detailed recommendations for how to carry out these tasks.

Since the NIST Framework already exists and financial institutions have already "designed their cybersecurity programs to implement the NIST Cybersecurity Framework,"[256] it would facilitate cohesion and mitigate duplicative efforts if data classification recommendations were based in part on the existing practices recommended by the NIST Framework. The three bodies could simply evaluate the recommendations made by the organizations the NIST Framework includes as informative references. Through dialogues, the three bodies could agree on which recommendations best accomplish common goals and publish a common list for use by the covered entities. Additional recommendations from other organizations could be included if agreed upon, but it would be ideal if some of the NIST Framework recommendations were included since they have already been widely implemented. It would also be helpful if explanations were provided regarding why certain recommendations were selected, as it could provide insight that would allow covered entities to adopt them in a more targeted manner. These would likely have to take the form of nonbinding policy guidance. However, agreement in this area would provide valuable guidance to covered entities regarding a critically important step that can potentially be very costly.

2. Writing the Playbook

The separate written policy requirements should be streamlined through consensus among the three bodies in order to create a single cohesive process and resultant document. Covered entities often have difficulty harmonizing the various requirements created by different regulatory regimes.[257] The complexity of the different requirements creates unnecessary financial costs in the form of time and resources spent on repetitive actions.[258] An approach that combines as many of the common steps and requirements as possible

253. *Id.*
254. *Id.*
255. *Id.*
256. SIFMA Comment Letter, *supra* note 19, at 2.
257. *What Is Regulatory Compliance?*, THRIVE NETWORKS (Oct. 27, 2011), https://www.thrivenetworks.com/blog/regulatory-compliance/ [http://perma.cc/Y4NM-2XPW] ("[M]any companies face multiple policies and regulations with regard to IT and data storage. This presents a challenge for most businesses . . . .").
258. *The Challenges of Managing and Tracking Compliance with Multiple Standards*, SYSNET GLOBAL SOLUTIONS, https://sysnetgs.com/2017/04/challenges-managing-tracking-compliance-multiple-standards/ [http://perma.cc/WQN3-KATQ] (last visited Aug. 24, 2018).

reduces these costs, saves time, and limits duplicative efforts.[259] Private sector companies offer products that are marketed as solutions to this problem; however, these products can be costly, especially for smaller entities.[260] And independently performing the analysis to create such a process also requires time and effort, which translates to financial costs.[261]

All three regulatory regimes require a written policy.[262] The elements they have identified as relevant to an acceptable written policy are largely similar and include such things as technical measures, monitoring mechanisms, access controls, training programs, and incident response plans.[263] The three bodies could maintain flexibility while still providing valuable guidance in the form of unofficial guidelines for creating a written policy. This could be relatively general and simply identify all of the elements that they would like the entity to consider in formulating the policy and identifying which regulation or regulations that element pertains to. This would help the covered entities adequately consider each element, identify which regulation requires it, and determine whether they are compliant.

Currently, the guidance in this area is either lacking or so general it essentially quotes from the regulation.[264] It would be beneficial if the three bodies produced a document similar to the *Security Series* promulgated by the U.S. Department of Health and Human Services.[265] In those documents, the relevant requirements are broken down into elements and questions for the covered entities to consider in formulating their policies and procedures.[266] They also identify what is required and what is optional.[267] Alternatively, some private sector organizations provide free templates outlining factors to consider in formulating different elements of a security policy.[268] Either of these types of document would be valuable to covered entities pursuing compliance.

The three bodies could engage in dialogues aimed at drafting such a document, or series of documents, and publish nonbinding guidelines according to their relevant statutes and authorities. This is desirable because the entities are best situated to identify and explain what they expect. Further, the discussions that would be necessary to create such a document would

259. *Id.*
260. *Id.*
261. *See id.*
262. *See supra* Part II.B.
263. *See supra* Part II.B.
264. *See General Data Protection Regulation: Guide for Processors*, COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, at 17 (2017), https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil_en.pdf [https://perma.cc/9DG5-XB96].
265. *See generally Security Standards: Administrative Safeguards*, 2 HIPAA SECURITY SERIES (Dep't of Health & Human Servs.), Mar. 2007, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf [https://perma.cc/YM5V-E5K9].
266. *Id.*
267. *Id.*
268. *See generally Router and Switch Security Policy*, SANS INST. (2014), https://www.sans.org/security-resources/policies/network-security/pdf/router-and-switch-security-policy [https://perma.cc/RYY7-BPXV].

help develop and share best practices and improve overall understanding of threats.[269] Finally, providing such a document would provide a more manageable and affordable path to compliance for all entities—particularly smaller ones that cannot afford to purchase private sector products that perform this analysis or perform it independently. Given the magnitude of the economic relationships, and the significance of financial institutions within those relationships, the impact of such a collaborative product would be far-reaching and should result in substantial economic benefits.

3. Decrypting Encryption

Encryption is another area where collaborative guidance could be beneficial. It is unclear precisely how encryption should be implemented to satisfy each set of regulations. A number of benefits would follow if common standards for encryption were established or endorsed by the regulatory bodies.[270] For example, standards would allow covered entities to shop for the most cost-effective product for their specific needs.[271] Standards also homogenize the level of security, so that individuals can implement approved cryptographic algorithms and key lengths and know the encryption is adequate.[272] In addition, standards contribute to the quality of products, by, for example specifying how features are implemented and requiring maintenance procedures to test whether the product continues to function correctly.[273] Finally, standards create common specifications that can also help limit knowledge and compatibility costs.[274]

The three bodies could approach this issue by engaging in a joint dialogue to identify the minimum standards they believe are necessary. Areas that could be addressed include algorithm strength, key length, and best practices for key management. As discussed above, algorithm strength can weaken over time,[275] which is why such dialogues should be ongoing. That way, any products of such dialogues can be updated or modified as circumstances require. Consensus guidance could be promulgated by each body using an appropriate vehicle according to the requirements and limitations of their statutory authority, keeping in mind that encryption is subject to change.

---

269. Jan Neutze, *Positive Steps on the Road Towards Harmonization of Global Cybersecurity Risk Management Frameworks*, MICROSOFT SECURE (Dec. 19, 2014), https://cloudblogs.microsoft.com/microsoftsecure/2014/12/19/nis-platform/ [https://perma.cc/5H8N-HFJE].

270. BARKER, *supra* note 200, at 12 ("Standards define common practices, methods, and measures/metrics. Standards provide solutions that have been evaluated by experts in relevant areas, reviewed by the public and subsequently accepted by a wide community of users. By using standards, organizations can reduce costs and protect their investments in technology.").

271. *Id.*

272. *Id.*

273. *Id.*

274. *Id.* at 13 ("Without standards, users may be required to become experts in every information technology (IT) product that is being considered for procurement. Also, without standards, products may not interoperate with different products purchased by other users. This could result in a significant waste of money or in the delay of implementing IT.").

275. *See generally supra* Part II.

As an alternative to defining standards themselves and revisiting them periodically, the bodies could identify organizations that promulgate encryption standards that meet their agreed criteria. Such criteria could include how often the standards organizations update their policies, what level of security the standards they recommend provide, and how widely those standards have been deployed. The three bodies could identify specific encryption standards based on similar criteria if they preferred. An additional benefit of this method is that there are organizations that certify the implementation of many of these standards. If the three bodies endorsed or certified these standards and organizations, covered entities would be able to more easily demonstrate an adequate implementation of encryption. It would also allow the regulatory bodies to more easily identify covered entities that meet their minimum standards.

CONCLUSION

Ultimately, there is no way to prevent all intrusions and cyber incidents from occurring. Therefore, the question is how resources should be allocated in a reasonable way to limit risk, mitigate damage, and protect consumers. Regulations are based on the judgments each regulatory body has made about the costs and benefits of sometimes competing values, reflecting the preferences of their constituencies. There will remain numerous areas where the regulations cannot be easily harmonized. But by identifying and working toward a consensus in the areas that can be harmonized, it is possible to shrink the areas of difference.

Doing as much as possible to weave the patchwork of regulations that currently exists into a cohesive set of practices would benefit every stakeholder. With reasonably consistent and clear paths to compliance, covered entities will be able to focus on implementing best practices, instead of identifying requirements. This will both lower the cost and improve the implementation of the practices established by the SEC, NYDFS, and EU. Consumers would be able to enjoy the protection contemplated by the regulations at the lowest cost. These three regulatory bodies can collaborate, using their expertise and resources to provide this guidance. This would more effectively mitigate the negative effects of cyber incidents, protect both the industries and consumers they oversee, and further the policies that they are statutorily charged with implementing.