Georgia State University Law Review

Volume 30
Issue 2 *Winter 2013*

Article 1

June 2014

The Efficacy of Cybersecurity Regulation

David Thaw

Follow this and additional works at: https://readingroom.law.gsu.edu/gsulr

 Part of the Law Commons

Recommended Citation
David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 Ga. St. U. L. Rev. (2014).
Available at: https://readingroom.law.gsu.edu/gsulr/vol30/iss2/1

This Article is brought to you for free and open access by the Publications at Reading Room. It has been accepted for inclusion in Georgia State University Law Review by an authorized editor of Reading Room. For more information, please contact mbutler@gsu.edu.

THE EFFICACY OF CYBERSECURITY REGULATION

David Thaw[***]

ABSTRACT

Cybersecurity regulation presents an interesting quandary where, because private entities possess the best information about threats and defenses, legislatures do—and should—deliberately encode regulatory capture into the rulemaking process. This relatively uncommon approach to administrative law, which I describe as Management-Based Regulatory Delegation, involves the combination of two legislative approaches to engaging private entities' expertise. This Article explores the wisdom of those choices by comparing the efficacy of such private sector engaged regulation with that of a more traditional, directive mode of regulating cybersecurity adopted by the

* Visiting Assistant Professor of Law, University of Connecticut; Affiliated Fellow, Information Society Project, Yale Law School. Funding for this project was provided by the U.S. Department of Homeland Security through the Institute for Information Infrastructure Protection (I3P), the Team for Research in Ubiquitous Secure Computing (TRUST), and the Rose Foundation. I owe special thanks to Deirdre K. Mulligan, Pam Samuelson, and Todd LaPorte, for their many years of advice and support in the development of my Ph.D. dissertation research, upon which this Article is in large part based. I also express thanks for the substantial assistance of Jennifer King and Aaron Burstein in the development and conduct of the Chief Information Security Officer interviews. This Article additionally benefited from the thoughtful comments of Ashok Agrawala, Jack Balkin, Derek Bambauer, Nicholas Bramble, Yale Braunstein, Brian Carver, John Chuang, Chris Hoofnagle, Leslie Levin, Peter Lindseth, Margot Kaminski, Elizabeth Khalil, Andrea Matwyshyn, Paul Mazzucco, Christina Mulligan, Mark Paulding, Gerry Stegmaier, the participants of the 2010 and 2012 Privacy Law Scholars Conference, the members of the Yale Law School Information Society Project, the participants in the Harvard-Yale-MIT-Columbia Cyberscholars Workshop Series, and my former fellow Ph.D. students at UC Berkeley's School of Information. The editors and staff of the *Georgia State University Law Review*, especially including Ashley Worrell and Andrea Iglesias, provided invaluable assistance and input in the finalization and production of this piece. Lastly, I express thanks to my father, the original Professor Thaw, for encouraging and supporting me in the long processes both of completing the training necessary to undertake this research and of completing a doctoral dissertation.

** This material is based in part upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006 CS 001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

Published by Reading Room, 2013

state legislatures. My analysis suggests that a blend of these two modes of regulating is superior to either method alone.

Federal regulation of cybersecurity through HIPAA, Gramm-Leach-Bliley, and the Federal Trade Commission's enforcement heavily involves private organizations subject to the regulation in the establishment of the actual practices and standards to which those organizations are held. By contrast, the state cybersecurity laws—a form of disclosure-based regulation that de facto achieves directive regulation—detail specific standards developed without industry input.

This Article compares the efficacy of those two modes of regulating using a mixed-methods empirical approach. Qualitative data based on interviews with Chief Information Security Officers (CISOs) at leading multinational corporations details the practical effects of how regulation drives cybersecurity practices. Analysis of quantitative data describing security breach incidents reveals that a blend of the two types of regulation is substantially more effective at preventing such incidents than is either method alone. These results provide insight into ways to mitigate the risks of deliberate regulatory capture while still leveraging the unique knowledge private entities have about what are the most salient cybersecurity threats and defenses.

TABLE OF CONTENTS

INTRODUCTION

Several years ago, while driving back from a job interview in Washington, D.C., I recall receiving (on my hands-free-enabled mobile phone) an "urgent" phone call from the issuing bank of my primary credit card. Upon returning the call, I learned that my credit card had been compromised and a new card needed to be issued—immediately. As a young cybersecurity scholar, I was curious and, inquiring further, was able to learn only that one of the payment processors with which the bank worked had experienced a massive security breach, and it was under investigation.

In 2008, payment card processor Heartland Payment Systems experienced a security breach[1] that resulted in the compromise of approximately 130 million consumer payment card records.[2] The compromise was the result of malicious software placed into Heartland's network that extracted the data describing payment card transactions and transmitted that information, including sensitive

1. Paul McNamara, *Banks Warn Customers as Debit-Card Processor Acknowledges Breach . . . "Larger than TJX?"*, NETWORKWORLD (Jan. 20, 2009, 10:03 AM), http://www.networkworld.com/community/node/37510.

2. *Incident 1518*, DATALOSSDB, http://www.datalossdb.org/incidents/1518-malicious-software-hack-compromises-unknown-number-of-credit-cards-at-fifth-largest-credit-card-processor (source requires registration to view).

financial account information, to an outside hacker.[3] The aftereffects of this breach included a substantial federal lawsuit and settlement fund,[4] substantial negative media coverage, and millions of customers (including the author) having to go through the process of waiting for a new card to arrive, checking statements for fraudulent transactions, and updating their information with vendors and automatic payment systems.[5] All because a vendor of very substantial size failed to employ reasonable security measures that could have prevented the hacker.

Cybersecurity is a complex topic in itself. Cybersecurity regulation, a topic of substantial policy and media attention over the past several years,[6] involves a complex mixture of state and federal regulation including varying regulatory approaches and varying degrees of scope. This Article seeks to accomplish three tasks: 1) describe the existing framework of cybersecurity regulation and contextualize that framework within existing scholarship on regulation,[7] 2) present the results of a mixed-methods empirical study evaluating the efficacy of the various regulatory approaches currently in use,[8] and 3) discuss how particular innovations in cybersecurity regulation result in a new, hybrid form of regulation not yet well-described in the literature.[9]

Unpacking "cybersecurity regulation" begins first with understanding to what the term "cybersecurity" refers. Cybersecurity and cyber-attack are increasingly common terms in public discourse, but there is surprising disagreement as to what precisely they refer. The terms are too-often used broadly to include all of electronic crimes,[10] military action,[11] domestic guard/homeland security

3. Brian Krebs, *Payment Processor Breach May Be Largest Ever*, WASH. POST (Jan. 20, 2009, 1:30 PM), http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html?hpid=topnews.

4. *See supra* note 2.

5. *Id.*

6. *See generally infra* notes 10–15.

7. *See* discussion *infra* Part I.A.

8. *See* discussion *infra* Parts III–IV.

9. *See* discussion *infra* Part II.

10. David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*,

activities,[12] corporate risk management,[13] financial security,[14] and a wide spectrum of other activities related to computers, the Internet, privacy, and other similar topics.[15] I do not suggest the term is misapplied to any of these topics, but rather that more precise terms would be helpful. To that end, for the purposes of this Article, I discuss those aspects of cybersecurity which refer to the information security measures[16] that custodians of consumer data[17] take to protect such sensitive information. Thus the scope of this Article is private law and regulation, and uses the term information security to describe those administrative, technical, and physical methods and practices

---

103 J. CRIM. L. & CRIMINOLOGY 907, 909 (2013).

11. *Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program*, *Hearing Before S. Comm. on Armed Servs.*, 113th Cong. 8 (2013) (statement of Gen. Keith B. Alexander, Commander, U.S. Cyber Command), *available at* https://www.hsdl.org/?view&did=733855.

12. Jennifer Martinez, *Senators Introduce Bill to Create Teams of Cyber Guardsmen at State-Level*, THE HILL (Mar. 22, 2013, 8:51 PM), http://thehill.com/blogs/hillicon-valley/technology/289931-senators-introduce-bill-to-create-teams-of-cyber-guards-at-state-level.

13. *See, e.g.*, *Defining the Future of Security and Risk*, CSO40 SECURITY CONFAB + AWARDS http://www.csoconfab.com/ehome/index.php?eventid=48220&tabid=95096&categoryid=345082&discountcode=NLP& (last visited Oct. 12, 2013) (describing generally the CSO40 conference of April 2–3, 2013 on "Defining the Future of Security and Risk").

14. Antone Gonsalves, *Largest Banks Under Constant Cyberattack, Feds Say*, CSO ONLINE (Nov. 2, 2012), http://www.csoonline.com/article/720584/largest-banks-under-constant-cyberattack-feds-say.

15. *See generally Digital Spotlight: Cybersecurity*, CSO, Feb.–Mar. 2013, *available at* http://resources.idgenterprise.com/original/AST-0082567_FEB4digi_0214i.pdf.

16. As noted by Professor Andrea Matwyshyn, "[r]eferring to all of information security, particularly in private sector contexts, as 'cybersecurity' is technically incorrect." Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NW. U. L. REV. 795, 817, n.99 (2013). Matwyshyn describes this misnomer as ignoring the aspects of physical security inherent in "holistic" protection of data maintained by an enterprise. *Id.* I concur with this assessment, and further suggest, as consistent with the Administrative/Technical/Physical breakdown described in Part II.B.3 of this Article, that such a characterization also overlooks the administrative aspects involved in protecting and securing information. *See also* Thaw, *supra* note 10, at 928 n.88 (discussing the distinction between purely-technical restrictions on computer usage and comprehensive administrative, technical, and physical restrictions thereon).

17. Generally, sensitive consumer data has been defined by federal and state statutes to include Personally Identifiable Information (PII), sensitive financial information, Protected Health Information (PHI), and certain other information subject to specific privacy protections (e.g., educational records of students). *See, e.g.*, 15 U.S.C. § 6809(4) (2012) (defining "nonpublic personal [financial] information"); CAL. CIV. CODE § 1798.80(e) (West 2012) (defining "Personal information"); *In re* TJX Cos., No. C-4227, 2008 WL 3150421, at *1 (F.T.C. Mar. 27, 2008) (defining "personal information" using language commonly found in similar FTC Consent Orders addressing privacy and information security issues); 45 C.F.R. § 160.103 (2013) (defining "protected health information").

involved in maintaining the regulatory standards imposed on private data custodians.

This Article introduces the concept of Management-Based Regulatory Delegation.[18] Cybersecurity presents an uncommon challenge in that the regulated entities—the private sector data custodians described above—not only generally possess expertise useful to the rulemaking process, but in fact possess superior knowledge regarding information security threats and defenses not otherwise available to regulators. Federal regulators leverage this knowledge not only voluntarily, but in some cases by *mandate*, engaging private entities in the rulemaking and *de facto* standards-setting processes.[19] Scholars variously have referred to this as a form of regulatory delegation.[20] In addition to including regulated entities at the proverbial "drafting table,"[21] regulators also engage in a process of management-based regulation under which the regulated entities themselves develop and adhere to their own individualized compliance plans.[22] While these plans must meet general guidelines, the regulatory goal becomes the development of and adherence to the plan, rather than compliance with specific technical obligations, directly.[23] Scholars have referred to this process by several names;[24]

18. Management-Based Regulatory Delegation is a mode of regulation under which administrative agencies, through legislative-mandated collaboration with regulatory stakeholders, promulgate regulations requiring regulated entities to develop plans designed to achieve certain aspirational goals laid out by the legislature. As discussed in Part II.B, Management-Based Regulatory Delegation is a combination of management-based regulation, in which administrative agencies promulgate requirements that regulated entities then develop, with regulatory delegation. Regulatory delegation is defined as a process in which administrative agencies enlist the expertise of the particular regulated party. Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L. J. 377, 386 (2006).

19. As discussed in Part II.B.3, adjudication by the Federal Trade Commission through settlements of its enforcement actions creates effective cybersecurity standards that currently are viewed by practitioners as having a prospective regulatory effect.

20. *E.g.*, Bamberger, *supra* note 18, at 385–86.

21. This is a level of engagement by regulated entities and other interested parties *far* in excess of anything required by informal rulemaking under the Administrative Procedure Act and possibly even exceeding that required under *formal rulemaking* guidelines. 5 U.S.C. § 553 (2006). While such a discussion is outside the scope of this paper, it is worth noting.

22. *See generally infra* notes 43, 84.

23. *See* Bamberger, *supra* note 18, at 386.

24. Cary Coglianese & David Lazer, *Management-Based Regulation: Prescribing Private*

this Article addresses it as management-based regulation. The net result of combining these two forms of regulation is what I describe as Management-Based Regulatory Delegation, a deliberate encoding of regulatory capture—both in the rulemaking and enforcement stages of the administrative process—to engage the superior knowledge possessed by regulated entities. And, indeed, the Chief Information Security Officers (CISOs) interviewed as part of this study describe how they participated in these processes most particularly with respect to the HIPAA Security Rule.[25]

I evaluate the efficacy of cybersecurity regulation by comparing the ability of those industries subject to Management-Based Regulatory Delegation models with those subject only to more directive regulatory models at preventing security breaches of sensitive consumer information. The latter category, which I describe as directive regulation, also presents an interesting finding in that the "directive" component results from an information disclosure-based regulation with a "safe harbor" provision that effectively becomes a directive mandate to employ the safe harbor.

This Article proceeds in four Parts. Part I contextualizes cybersecurity regulation within the existing scholarship on regulatory frameworks and identifies how those frameworks fail to describe cybersecurity regulation adequately.[26] Part II provides a descriptive account of a new hybrid form of regulation emerging in cybersecurity and proposes an alternate framework for categorizing regulation.[27] Using this framework, it divides existing cybersecurity regulation into two categories for comparative analysis. Part III presents the results of a quantitative study of security breach incidence which suggests that blending traditional directive regulation with

---

Management to Achieve Public Goals, 37 LAW & SOC'Y REV. 691, 692 n.1 (2003) (describing management-based regulation as a concept variously referred to as "'enforced self-regulation' (Braithwaite 1982), 'mandated self-regulation' (Bardach & Kagan 1982; Rees 1988), 'reflexive' regulation (Orts 1995), or 'process-based' (Gunningham & Grabosky 1998) and 'systems-based' (Gunningham 1996; Gunningham & Johnstone 1999) standards").

25. *See infra* Part IV.B.2.

26. *See* discussion *infra* Part I.

27. *See* discussion *infra* Part II.

Management-Based Regulatory Delegation is superior at breach prevention than is either method alone.[28] Part IV provides a practical account of the effects of each type of regulation from the views of CISOs and suggests how blending the two modes of regulating can offset the various weaknesses inherent within each mode alone.[29]

I. DEVELOPING A THEORY OF REGULATORY CLASSIFICATION

Information security laws have not yet been classified in the literature on regulation. Understanding these laws' character and function is critical to evaluating their efficacy and considering both how to improve them and what lessons they may have for regulation in other industrial sectors.

Information security regulation is unique at the federal level in that it heavily involves private parties both in the creation of standards and in the adherence to those standards through individualized compliance plans.[30] This blend, which I describe as Management-Based Regulatory Delegation, is a combination of theories advanced on regulatory delegation[31] and management-based regulation.[32]

A. A Brief Summary of Information Security Regulations

I discuss the various information security regulations considered in this Article in more depth later when developing a method of classifying those regulations for empirical comparison. Situating this work within the existing literature does, however, require some reference to these laws and regulations, and I provide here a brief overview of the main pieces of the information security regulatory puzzle.

---

28. *See* discussion *infra* Part III.
29. *See* discussion *infra* Part IV.
30. *See* Bamberger, *supra* note 18, at 386.
31. *See id.*
32. *See* Coglianese & Lazer, *supra* note 24.

1. Federal Information Security Regulation

Information security regulation at the federal level comprises three primary components. The first, respecting the financial sector, is the Gramm-Leach-Bliley Act (GLBA).[33] GLBA provides both the Federal Trade Commission (FTC) and various agencies within or associated with the Department of the Treasury authority to promulgate and enforce regulations regarding information security measures financial institutions must employ to protect the sensitive information they maintain on behalf of consumers.[34] GLBA mandates a certain level of involvement by specific parties who must be consulted during the rulemaking process.[35]

The second, respecting the healthcare sector, is the Health Insurance Portability and Accountability Act (HIPAA),[36] which provides the Department of Health and Human Services the authority to promulgate and enforce regulations regarding information security measures healthcare entities and their associates must employ to protect the sensitive information they maintain on behalf of patients, research subjects, and individuals whose medical information they collect/maintain.[37]

Finally, the third component is the enforcement "jurisprudence" of the FTC under its "unfair and deceptive acts or practices" authority pursuant to Section 5 of the FTC Act.[38] Under this authority, the FTC has engaged in a variety of enforcement actions asserting that various information security practices of entities subject to its jurisdiction were unfair, deceptive, or both, in that they failed to employ

33. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., 16 U.S.C., 18 U.S.C., and 29 U.S.C.).

34. Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. §§ 6804, 6805 (2012).

35. *Id.* § 6804(a)(2).

36. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.).

37. 42 U.S.C. § 1320d-2(d)(1) (2006).

38. 15 U.S.C. § 45(a)(1) (2006).

reasonable information security measures to protect the sensitive personal information of those entities' consumers.[39]

2. State Information Security Regulation

At the state level, legislatures beginning in 2003 passed laws requiring entities losing control (experiencing security breaches) of certain "personal information" describing individuals to notify those individuals (and sometimes state regulatory authorities) of the breach, unless the data lost was encrypted.[40] As of August 2012, forty-six states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands have such laws.[41] This "encryption safe harbor," under which an organization is exempt from disclosure if the data were encrypted, has the effect of transforming an information disclosure-based regulatory regime into a directive regulatory regime *de facto* requiring organizations to encrypt sensitive consumer data.[42]

3. Other Information Security Regulations

It is worth noting to the reader that other information security regulations exist, both at the state and federal level, addressing protection of consumer information and the responsibilities of private entities. These include information security regulations promulgated by the Internal Revenue Service, by the Massachusetts Department of Consumer Affairs and Business Regulation, and laws passed by various states concerning maintenance and disposal of consumer information. Additionally, the Department of Defense (DoD) and the Securities and Exchange Commission (SEC) have promulgated regulations and issued guidance concerning the information security

39. *See* discussion *infra* Part II.B.3.

40. CAL. CIV. CODE § 1798.29 (West 2013).

41. *State Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last updated Dec. 26, 2013).

42. See *infra* Part IV.

of contractors with which the DoD does business and the disclosures publicly-traded companies should make to investors.

The interviews with CISOs, my professional experience, and my impression of my current and former colleagues' experiences in this regard all suggest that these "ancillary" regulations do not (yet) have a substantial impact on information security practices respecting consumer data. Thus at least at this stage of research, they are outside the scope of consideration. I include them here for the reader's general information.

B. Coglianese and Lazer's Model

Cary Coglianese and David Lazer propose that regulatory models can be grouped into three discrete categories based on the stage in an organization's production process at which the regulation attempts to intervene.[43] They suggest that intervention may occur when planning production ("planning stage"), implementing production ("acting stage"), or determining the final outputs of production ("output stage").[44] Each of these stages, according to the Coglianese and Lazer model, corresponds to a different type of regulation. The sections that follow discuss these stages in detail.

As defined by Coglianese and Lazer, technology-based regulation is an approach in which regulatory standards govern the means of production.[45] Occurring at the implementation (or "acting") stage, it specifies technologies that must be employed or processes that must be followed.[46] Technology-based regulation in the pollution control context, for example, could specify certain types of emissions control technologies that must be employed. In the information security context, technology-based regulation could specify that custodians of sensitive personal information must employ specific security

43. Coglianese & Lazer, *supra* note 24, at 693–94.
44. *Id.* at 694.
45. *Id.*
46. *Id.*

measures such as anti-virus and anti-malware software on their systems.

Performance-based regulation is an approach in which regulatory standards govern the final state or result of a production process.[47] Occurring at the output stage, regulation of this form specifies the characteristics of products or services that must be achieved or avoided. Unlike technology-based regulation, performance-based approaches are generally agnostic as to the means by which the producer achieves the specified goal. Performance-based regulation in the pollution control context, for example, could specify limits on the quantity of pollutants a manufacturing facility could release into the atmosphere. In the information security context, performance-based regulation could specify that entities retaining payment card information must not lose control of (e.g., have stolen) consumers' payment account information.

Management-based regulation is an approach in which regulatory standards address conditions that must be met during the planning stage of a productive process—before manufacture of a product or provision of a service begins.[48] It most commonly requires organizations to conduct risk assessments, produce risk management plans, or both.[49] Unlike technology-based regulation or performance-based regulation, management-based regulation does not begin from a premise of requiring an organization to engage in a pre-specified process or achieve a pre-specified goal. Rather, it mandates the undertaking of a general *type* of process (e.g., a risk assessment) and possibly adherence to the results of that process (e.g., a risk management plan). Management-based regulation may even specify general areas that these analyses and plans must address. The

47. *Id.*

48. *Id.* at 694–95.

49. As noted by Coglianese and Lazer, management-based regulation may also require organizations to implement and adhere to the risk management plans they develop. Coglianese & Lazer, *supra* note 24, at 707–11. Such requirements structurally overlap both with technology-based regulation and with performance-based regulation in that they effectively specify approaches that must be employed and end conditions that must be achieved. The specifications of these technology and performance requirements will obviously differ as the organizations self-define the guidelines.

"compliance" element, however, is the actual development of the plan and the "compliance details" are specified by the organization (through its analyses/plans) rather than by the regulator.

Management-based regulation in the pollution control context could, for example, require that manufacturing plants conduct analyses to determine their current levels of pollutants and develop plans to reduce those levels. In the information security context, management-based regulation could require that organizations maintaining sensitive personal information conduct risk analyses of their information systems and develop risk management plans to reduce the probability of those systems being compromised and individuals' sensitive information being lost.

Coglianese and Lazer's model focuses heavily on the timing of regulatory intervention as the spectrum along which classes of regulation are differentiated.[50] It strictly links the timing of regulatory intervention to the functional method of regulation. The resultant typology is incomplete for the purpose of classifying information security regulation.

C. The Role of "Timing"

To understand the ways in which Coglianese and Lazer's typology overlooks certain types (and potential types)[51] of information security regulation, it is first necessary to understand what constitutes a security "good" or "output." Coglianese and Lazer define outputs in the context of traditional industrial production.[52] They consider outputs to "include both private and social goods, that is, saleable products or services (private goods) as well as the positive and negative externalities (social goods and bads) that affect society."[53]

---

50. *See generally* Coglianese & Lazier, *supra* note 24.

51. Discussing "potential types" of information security regulation is critical at this juncture both because the existing regulation only addresses the protection of certain types of information and because there are strong indications that federal regulators consider this to be a critical and urgent issue. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011).

52. Coglianese & Lazer, *supra* note 24, at 693.

53. *Id.*

Unlike traditional industrial production involving the manufacture of physical products (e.g., foodstuffs) or the provision of professional services (e.g., management consulting services), information security does not have well-defined "outputs" of the type described above. In traditional industries, these well-defined outputs come into being at an end stage in the production lifecycle as a result of steps designed to result in the desired output.[54] In the context of information security, the state of keeping an information system secure can be considered a good or service. A single security violation, however, does not mean the "good" has not been produced or the "service" not delivered. Information security, as identified by several respondents, is an exercise in risk mitigation, not risk prevention.[55] Thus, many of the deliverable "goods" or "services" are defined by engaging in activities that are likely, but not guaranteed, to mitigate system compromise.[56] It is therefore the act of engaging in those activities, *not* the result of the activities themselves, that constitutes the output for information security. Understanding this distinction between traditional goods and information security is critical to understanding how to evaluate information security regulation.

A second critical difference is the means by which success or failure is evaluated. Coglianese and Lazer consider three industrial activities as examples in discussing their typology: food safety, pollution, and industrial safety.[57] Information security does somewhat resemble these traditional areas in that each of them is associated with producing a physical good, rather than being the primary object of production themselves.[58] Unlike these three

54. *See id.* Figure 1 at 694.

55. Most of the CISOs interviewed described their job and the task of information security as risk management. One CISO, for example, even went so far as to describe their job as "[r]isk management, not security at all." David Bernard Thaw, Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets 8, n.16 (Spring 2011) (Ph.D. dissertation, University of California, Berkeley) (on file with Georgia State University Law Review).

56. *Id.* at 8.

57. Coglianese & Lazer, *supra* note 24, at 696–700 (discussing authors' typology).

58. Thaw, *supra* note 55, at 8 n.18 ("Information security is, in large part, a process/procedure/goal (to protect assets) associated with some other productive activity.").

categories, however, information security lacks well-defined metrics by which to evaluate outcomes.[59] The lack of well-defined metrics makes it difficult to evaluate information security outcomes strictly at the output stage.

Professionals and regulators evaluate information security outcomes as a function of whether certain practices are followed, not whether those practices are effective. This approach is, in part, due to an inability to measure the efficacy of such practices because demonstrating success is often an exercise in "proving a negative."[60]

As a result, the characteristics used to evaluate "success" in information security reside not only at the output stage, but also at the acting and planning stages of Coglianese and Lazer's typology. In the case of environmental pollution, for example, success ultimately can be evaluated by measuring a well-defined output condition—what pollutants are (or are not) released. In the information security context, by contrast, the lack of a successful attack does not indicate that security measures were effective—exploitable system vulnerabilities simply may not have come under attack during the evaluation period. Thus the measure of success[61] is not always directly linked to a goal or output in the traditional sense, and goals and outputs, therefore, must be considered more broadly with respect to information security. Specifically, as it pertains to this section, such breadth includes considering outputs to exist both at the planning and at the acting stages of Coglianese and Lazer's typology. The refinements I propose address this disconnect by redefining the final stage of production to include outputs that occur

59. *Id.* at 8 n.19 ("Several of the CISO respondents lamented the lack of available metrics particularly as it pertained to justifying information security expenditures to management.").

60. *Id.* at 8 n.22 ("A few of the CISO respondents specifically expressed part of the difficulty in their job being the process of proving to management that resources allocated to information security were well-spent given the *lack* of something occurring—essentially placing them in the position of having to 'prove a negative.'").

61. *Id.* at 9 n.23 (differentiating the measure of success "from the measure of *compliance*, which *can* be measured at all three stages in the industrial production cycle—a fact obviously central to Coglianese and Lazer's analysis").

chronologically at other stages, but are information security outcomes as defined in this section.

I discuss this concept, which I call the Information Security Production Lifecycle, in the section that follows. Understanding the role of timing is critical to understanding the shortcomings of Coglianese and Lazer's typology for categorizing information security regulation. Understanding timing in this context requires understanding how the Information Security Production Lifecycle differs from the production lifecycle for more traditional goods. The section that follows identifies these differences, thereby setting up the background to discuss the specific shortcomings of Coglianese and Lazer's typology.

1. The Information Security Production Lifecycle (ISPL)[62]

Information security has the interesting characteristic of being both an economic good and a process of producing that good. It is a good in the sense of providing definable (and sometimes measurable) outcomes. The process of producing these outcomes, however, is also an element of information security. In other examples, such as manufactured products, the process to produce the product is distinct from the product itself and may employ technologies unrelated to the final product. Information security differs in that elements of the productive process to achieve information security outcomes are also elements of the outcomes themselves.

Put differently, the means of reaching an information security outcome are as much an information security "product" as is the outcome itself. For example, an information security outcome may be to reduce the incidence of computers being hijacked for use in a "botnet,"[63] and a means for achieving that outcome may be the deployment of system security software including anti-virus software with heuristic detection. The deployment of such software is also a

62. The text accompanying this part is largely attributable to Thaw, *supra* note 55, at 7–12.

63. *Botnet Definition*, TECH TERMS COMPUTER DICTIONARY, http://www.techterms.com/definition/botnet (last updated June 9, 2010).

recognized information security goal, or "product," independent of the organization's specific focus on countering a particular or general threat of machine hijack.[64]

In the following three sections, I propose a friendly refinement to the stages of production examined by Coglianese and Lazer. The purpose of this refinement (and renaming) is specific to information security and to industries that may resemble its production characteristics.[65]

a. Design/Planning Stage

The design and planning stage is that point in the ISPL when decisions about how to implement information security measures are made. Coglianese and Lazer refer to this as the "planning" stage in organizational production and that stage at which management-based regulation is targeted.[66] Many of the characteristics they associate with management-based regulation are applicable to the design and planning stage defined here. As applied to information security, however, their model does not anticipate planning activities that require specific implementation choices, whereas the effects of some information security regulations do require that such decisions be made at the planning stage.[67] This differs from Coglianese and Lazer's conception of management-based regulation, which they describe as "shar[ing] some of the advantages of performance-based regulation in that it allows firms the flexibility to choose their own control or prevention strategies."[68]

---

64. INT'L INFO. SYS. SEC. CERTIFICATION CONSORTIUM, CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CANDIDATE INFORMATION BULLETIN 18 (2012) (noting that preventing or responding to "attacks (e.g., malicious code, zero-day exploit, denial of service)" and "[i]mplement[ing] and support[ing] patch and vulnerability management" are critical to security operations).

65. The following should not be interpreted to suggest that the stages of production examined by Coglianese and Lazer should be refined in the context of traditional industries; in fact, as of the time of this writing I have not yet identified any other industries bearing the characteristics of information security that suggest these refinements.

66. Coglianese & Lazer, *supra* note 24, at 693–94.

67. *See, e.g.*, 201 MASS. CODE REGS. 17.00 (2013).

68. Coglianese & Lazer, *supra* note 24, at 702; Thaw, *supra* note 55, at 10 n.28 ("[M]anagement-based regulation mandates *that* firms engage in planning activities but does *not* specify how those

b. Implementation/Maintenance Stage

The implementation and maintenance stage is that portion of the ISPL encompassing activities giving effect to security measures, responding to security incidents/events, and other activities related to the deployment and upkeep of security plans. This includes the implementation and maintenance not only of technical security measures, but also of administrative and physical security measures as well. Coglianese and Lazer refer to this as the acting stage.[69] In their typology, it is that stage at which technology-based regulation is targeted.[70]

c. Efficacy/Output Stage

The Efficacy/Output Stage is that portion of the ISPL encompassing definable outcomes. I suggest that such definable outcomes are used to evaluate success at, and exist at, all three stages of the ISPL. These outcomes include both: (1) *procedural* outcomes or those as steps taken to mitigate risk; and (2) *measurable* outcomes or those for which an external metric can evaluate success.[71] Together, these two categories define the Efficacy/Output Stage.

This is markedly different from Coglianese and Lazer's approach, which considers the output stage (as they call it) to be that stage of production in which outputs (both good and bad) come into being.[72] Outputs in traditional industries come into being at the end of a production cycle as the result of some process or steps designed to

---

activities must implement mechanisms to achieve regulatory goals.") (emphasis in original).

69. Coglianese & Lazer, *supra* note 24, at 694.

70. *Id.*

71. Thaw, *supra* note 55, at 11 n.30 ("'External metric' in this context refers to something not an element of the information security *process*, such as a data breach, electronic break-in, network compromise, or other failure of security. It can also represent positive outcomes, such as the successful detection of and defense against an attack, or the investigation of an incident and apprehension of the perpetrator of that incident. This distinction is important as it highlights the difference between traditional outcomes (appropriate to be measured and examined at the output/efficacy stage) and information security outcomes which, as discussed above . . . exist at all stages of the ISPL.") (emphasis in original).

72. Coglianese & Lazer, *supra* note 24, at 693–94.

result in those outputs. In the context of information security, I argue that many outputs are the actual process or steps themselves, and come into being chronologically before the "end" stage of production.

The deployment of system security software, for example, is a recognized procedural outcome that occurs chronologically at the Design/Planning (as to software selection) and Implementation/ Maintenance (as to operation/updating) Stages. For the purposes of characterizing certain regulation, however, it makes sense to consider this goal as an outcome rather than as a process to achieve an outcome. The choice of approach will depend on the structure of, and purpose behind, the regulation. A regulation that seeks to implement system security software to achieve some other specific goal, such as the protection of personal information, suggests treating the deployment of system security software as a process, not an outcome. A regulation that seeks to implement system security software to mitigate negative externalities caused by the absence of that software, however, suggests treating the deployment of such software as an outcome. This distinction, while perhaps overly fine, is important in characterizing the function of information security regulation and is thus a necessary refinement to Coglianese and Lazer's approach.

Measurable outcomes are the result of processes or steps. The most straightforward example is security incidents. While these are negative outcomes, they are definable, measurable events. These types of occurrences are always outcomes and more closely align with the traditional concept of production outputs. Measurable outcomes and procedural outcomes together define the Efficacy/Output Stage for the purposes of characterizing information security regulation.

D. Coglianese and Lazer's Model is Incomplete

First, technology-based regulation is under-inclusive. By linking strictly to regulation of methods and means at the production stage,[73] Coglianese and Lazer's conception of technology-based regulation ignores regulatory instruments that address methods and means, but do so at a different stage of the production cycle. Consider a case where the technology is itself the output of the productive process. If the "good" in question is an authentication mechanism to allow accountholders electronic access to their financial accounts, regulatory intervention governing the final output product would regulate "technology" as much as would regulations aimed at the process of developing the authentication mechanism. To be sure, the latter is a necessary part of information security regulation, and as identified by the International Information Systems Security Certification Consortium ((ISC)^2), security considerations must be a part of the software development life cycle.[74] However, to limit the term "technology-based regulation" only to those events occurring during production fails to capture fully the ways in which technology may be regulated.

Second, performance-based regulation fails to consider circumstances where the target of the regulation is output conditions, but aspects of the regulation's mechanism produce an effect regulating technology or means during the production stage. Perhaps the most notable examples of this phenomenon are the Security Breach Notification (SBN) statutes, which led to the rapid adoption of technologies to encrypt sensitive personal information stored on removable or portable media.[75] This adoption appears largely to result, as discussed in Part III, from provisions in most jurisdictions'

73. *Id.* at 693–95.

74. INT'L INFO. SYS. SEC. CERTIFICATION CONSORTIUM, *supra* note 64, at 12 (noting that "[s]ecurity of the software environment"—including "[o]peration and maintenance" and "[c]hange management"—are essential components of "security in the software development life cycle").

75. Thaw, *supra* note 55, at 13, 105–06.

SBN statutes providing "safe harbors" from notification requirements if the compromised or lost data was encrypted.[76]

Third, Coglianese and Lazer's typology ties management-based regulation to the planning stage of production. Unlike with technology-based or production-based regulation, Coglianese and Lazer's typology does consider some regulatory activity outside the planning stage. Specifically, they consider that management-based regulation may mandate both planning activities *and* implementation of the activities specified by the plan.[77] This distinction is important, and allows their typology to consider forms of regulation like HIPAA, which mandate both that Covered Entities develop security plans and that they adhere to those plans.[78]

Enforcement such as that by the FTC however, as discussed in greater detail in Part II, presents a hybrid model of management-based regulation not captured by Coglianese and Lazer's typology. FTC enforcement actions result both in specific compliance orders and in a requirement to conduct regular information security (and/or privacy) assessments.[79] Unlike the assessments conceived under traditional management-based regulation, FTC-ordered assessments are *reactive* in nature instead of *proactive*.[80] Furthermore, the effective goals of those assessments are tied *ex ante* (the assessment) to those specific compliance objectives.[81]

The effective result is a hybrid style of management-based regulation involving assessments which begin from a different chronological point than described by Coglianese and Lazer's traditional model. Additionally, these consent decrees have a broader effect, as the specific compliance elements thereof often are considered to become *de facto* regulations to which other firms are subject, as discussed further below in Part II.[82]

---

76. *Id.*
77. *See* Coglianese & Lazer, *supra* note 24, at 706.
78. 42 U.S.C. § 1320d-2(d)(1) (2006).
79. *See* discussion *infra* Part II.B.3.
80. *Id.*
81. *Id.*
82. *Id.*

E. Reconsidering Regulatory Classification for Information Security

Certain information security regulatory structures rely on a fundamental concept of "reasonable security."[83] This concept, not unlike other forms of regulation, presumes that a one-size-fits-all approach to regulating is not optimal[84] and looks to the regulated industrial sectors (and their constituent entities) to exercise some professional judgment as to what choices are reasonable to meet the compliance requirements of the regulations. HIPAA and GLBA are the two most prevalent examples of this type of regulation in the information security space.

The concept described above bears general resemblance to Coglianese and Lazer's conception of management-based regulation. However, as discussed above, their definition fails to adequately capture the character of these laws for the purposes of understanding information security regulation. Part II discusses an alternate approach to understanding HIPAA and GLBA (respectively). This groundwork explains what HIPAA and GLBA are—regulatory frameworks that seek input from industry professionals in the establishment of their regulations. To fully understand the effects of this style of regulation on the organization, it is necessary to distinguish these frameworks from other regulatory frameworks with an apparently similar notice-and-comment rulemaking process.

I propose considering regulation in three categories: (1) traditional legislation that is merely directive, and does not provide rulemaking authority to administrative agencies;[85] (2) legislation that delegates rulemaking authority to administrative agencies but does not specify deference to industry;[86] and (3) legislation that delegates rulemaking authority to administrative agencies and specifies that those agencies *must* consult with industry stakeholders during the rulemaking

83. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1173(d), 100 Stat. 2025–26 (codified as amended at 42 U.S.C. § 1320d-2(d) (2006)).

84. *See* Bamberger, *supra* note 18, at 387 ("One-size-fits-all rules cannot easily account for the ways in which risk manifests itself differently across firms.").

85. *See* discussion *infra* Part I.E.1.

86. *See* discussion *infra* Part I.E.2.

process and in some cases must defer to industry standards.[87] The first category describes regulation, as discussed in Part IV, that interferes with the exercise of professional discretion by information security professionals. The third category describes regulation that encourages reliance on the discretion of information security professionals.

1. Directive Legislation

Directive legislation is that which does not involve a rulemaking process by an administrative or other agency. The legislation itself establishes (usually straightforward) standards governing regulated entities and leaves no details to administrative agencies. Two examples of such legislation are the Video Privacy Protection Act (VPPA)[88] and the Electronic Communications Privacy Act (ECPA).[89] The VPPA specifies limitations on the disclosure of personally identifiable information[90] of consumers who rent, purchase, or subscribe to other goods and services from a video tape service provider.[91] The restriction is straightforward, and the statute neither prescribes any rulemaking authority nor references the involvement of an administrative agency in the regulatory process.

ECPA operates in a similar fashion. It makes the unlawful interception[92] of wire communications a felony[93] and specifies precisely what constitutes unlawful interception and what exceptions exist.[94] Like the VPPA, ECPA neither prescribes rulemaking

87. *See* discussion *infra* Part I.E.3.

88. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified as amended at 18 U.S.C. §§ 2710–11 (Supp. 2013)).

89. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–11 (2012)).

90. Interestingly, the VPPA provides one of the earlier definitions of "personally identifiable information"—one that far predated those codified in SBNs. The VPPA's definition is simple but ambiguous, "includ[ing] information which identifies a person as having . . . obtained specific video materials or services from a video tape service provider[.]" Video Privacy Protection Act of 1988 § 2.a.2(3).

91. 18 U.S.C. § 2710(b)(1) (Supp. 2013).

92. 18 U.S.C. § 2511(1)(a) (2012).

93. *Id.* § 2511(4)(a).

94. *Id.* § 2511(2).

authority for any administrative agency—even the Federal Communications Commission (FCC)—nor references the involvement of any such agency, except as to referencing previously existing FCC rules for descriptive purposes.[95]

SBNs, which I discuss extensively in Part II, also bear this character. They share a common framework of describing a triggering condition, which if met requires notification of a loss of control of certain types of personal information, unless certain exceptions (e.g., the data was encrypted) apply.[96] With the exception of deferment to law enforcement agencies as to delaying notification obligations, these statutes generally do not involve administrative agencies at all. When they do, it is generally limited to a centralized reporting requirement and not a rulemaking component. This type of regulation has substantial implications for information security professionalism in organizations as discussed in detail in Part IV.

2. Traditional Notice-and-Comment Rulemaking

The traditional "notice-and-comment" rulemaking process is one with which regulatory practitioners would likely be familiar. Congress crafts legislation specifying general goals, and directs an administrative agency to engage in a "rulemaking" process to fill in the details.[97] The agency publishes notices to this effect in the Federal Register, inviting the public (and more specifically, interested parties) to submit comments.[98] The agency then considers these comments and drafts regulations pursuant to the authority granted to it by Congress.[99] It publishes those regulations and their effective date in the Code of Federal Regulations, and after the effective date, entities subject to the regulations are responsible for compliance therewith.[100]

---

95. *See generally* § 2511.
96. Thaw, *supra* note 55, at 34.
97. *See generally* 5 U.S.C. § 553 (2006).
98. *Id.* § 553(b).
99. *Id.* § 553(c).
100. *See* Richard B. Stewart, *The Reformation of American Administrative Law*, 88 HARV. L. REV.

Many regulations across a wide variety of substantive fields follow this model. In the consumer/privacy regulatory space, two notable examples are the Children's Online Privacy Protection Act (COPPA)[101] and the Fair Credit Reporting Act (FCRA).[102] COPPA, for example, specifies that the FTC shall implement regulations to ensure various protections with respect to children's usage of websites.[103]

These regulations require the FTC to, subject to the requirements of the Administrative Procedure Act (APA),[104] promulgate regulations to achieve the intent specified above. The APA does not specifically require the FTC (or any other federal agency) to defer to the judgment of private industry or professionals in the promulgation of those rules. FCRA has similar requirements.[105]

Delegating these responsibilities to the FTC (and other financial regulatory agencies) makes sense. Developing rules for consumer notification procedures is a core competency of the Commission.[106] Likewise, developing rules governing the use of consumer reports and related financial information is a core competency of the Commission and the other financial regulatory agencies referenced in FCRA.[107]

On the surface, HIPAA and GLBA appear to fit this model. There is, however, a fine but critical difference between the way in which this process was implemented with respect to HIPAA and GLBA as

---

1673, 1683–88, 1775 n.500 (providing a thorough discussion of the administrative agency rulemaking process, with specific relevant emphasis at the pages noted, and a critique of this process).

101. Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2681 (codified as amended at 15 U.S.C. §§ 6501–06 (2006)).

102. Fair Credit Reporting Act, Pub. L. 91-507, 84 Stat. 1114 (1970) (codified as amended at 15 U.S.C. §§ 1681–81u (2006)).

103. 15 U.S.C. § 6502(b).

104. Administrative Procedure Act, Pub. L. 79-404, 60 Stat. 237 (1946) (codified as amended at 5 U.S.C. §§ 500–04 (2006)).

105. *See, e.g.*, 15 U.S.C. §§ 1681a(q)(3), 1681b(g)(5), 1681c(h)(2), 1681i(e)(4), 1681j(a)(1)(C)(i) (providing various federal regulatory agencies' rulemaking authority and prescribing mandatory rulemaking processes that those agencies must engage in to fill in gaps not addressed specifically by statute).

106. Thaw, *supra* note 55, at 26.

107. *Id.*

compared to other traditional notice-and-comment rulemaking. The difference lies in Congress's command to the regulatory agencies with respect to the rulemaking process and the differences in the core competencies of the relevant agencies at the time HIPAA and GLBA were passed.[108]

3. Notice-and-Comment Rulemaking with Deference to Industry (Regulatory Delegation)

There is a fine but critical distinction between traditional notice-and-comment rulemaking under the APA and the rulemaking requirements Congress established for HIPAA and GLBA. In each of these cases, Congress specifically called out groups with whom the administrative agencies promulgating the rules must consult.[109] Those groups comprised representatives of industry and other key stakeholders who, notably, *did* have privacy and information security competencies that the respective HIPAA and GLBA agencies were unlikely to have (at that time). Additionally, these stakeholders had access to unique information about information security threats and the efficacy of various defenses at addressing those threats likely unique to the stakeholders and not otherwise readily available to the regulators. In the case of the HIPAA Privacy Rule, for example, Congress specifically required that: "(d) Consultation.—In carrying out this section, the Secretary of Health and Human Services shall consult with—(1) the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)); and (2) the Attorney General."[110] In

108. In the case of HIPAA, the Department of Health and Human Services; in the case of GLBA, the federal financial regulatory agencies charged with its implementation. *See infra* note 204.

109. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264(d), 110 Stat. 2033, 2034 (codified as amended at 42 U.S.C. § 1320d-2 (2006)); Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., 16 U.S.C., 18 U.S.C., and 29 U.S.C.).

110. Health Insurance Portability and Accountability Act § 264(d) (applying this consultation requirement to the regulatory authority afforded HHS in § 264).

the case of the HIPAA Security Rule,[111] Congress's command was even more explicit:

> In complying with the requirements of this part [which includes § 1173(d)], *the Secretary shall rely on the recommendations of the National Committee on Vital and Health Statistics* established under section 242k(k) of this title [the Public Health Service Act], and shall consult with appropriate Federal and State agencies and private organizations. The *Secretary shall publish in the Federal Register any recommendation* of the National Committee on Vital and Health Statistics regarding the adoption of a standard under this part.[112]

The National Committee on Vital and Health Statistics (NCVHS) comprises key stakeholders in the health and health information policy fields from industry, government, and academia.[113] The current committee comprises

> 18 individuals distinguished in the fields of health statistics, electronic interchange of health care information, privacy and security of electronic information, population-based public health, purchasing or financing health care services, integrated computerized health information systems, health services research, consumer interests in health information, health data standards, epidemiology, and the provision of health services.[114]

111. § 1173(d), 110 Stat. at 2025–26 (codified as amended at 42 U.S.C. § 1320d-2(d) (2006)) (authorizing regulations set forth at 45 C.F.R. Parts 160 and 164). *See infra* notes 189–193.

112. § 1172(f), 110 Stat. at 2024 (codified as amended at 42 U.S.C. § 1320d-1(f) (2006)) (emphasis added) (§ 1172(f) applies to HIPAA § 1173(d) per the specifications of HIPAA § 1172(c)(3)(A)(ii) (codified at 42 U.S.C. § 1320d-1(c)(3)(A)(ii) (2006))).

113. Nat'l Comm. on Vital & Health Statistics, *Introduction to the NCVHS*, NVCHS, http://www.ncvhs.hhs.gov/intro.htm (last updated Mar. 13, 2006). *See also* 42 U.S.C. § 242k(k)(2) (2012).

114. Nat'l Comm. on Vital & Health Statistics, *supra* note 113. The full committee membership is available online at http://www.ncvhs.hhs.gov/members.htm (last updated Jan. 6, 2014).

As noted above, the Committee is also responsible for assisting the Secretary in promulgating rules relating to the HIPAA "Security Rule,"[115] which governs the information security requirements for the interchange of health-related information.[116]

In the case of GLBA, Congress's command is not as clear. The Act requires that:

> (b) . . . each [of the 8 GLBA regulators] shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
> (1) to ensure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[117]

It specifies that, with respect to rulemaking in this regard:

> (1) Rulemaking
>
> The Federal banking agencies, the National Credit Union Administration, the Secretary of the Treasury, the Securities and

115. 42 U.S.C. § 1320d-2(d).

116. 42 U.S.C. § 242k(k)(5)(A)(iv)-(v), (vii) (requiring the Committee to "advise the Secretary" "with respect to the design of and approval of health statistical and health information systems concerned with the collection, processing, and tabulation of health statistics within the Department of Health and Human Services, with respect to the Cooperative Health Statistics System established under subsection (e) of this section, and with respect to the standardized means for the collection of health information and statistics to be established by the Secretary under subsection (j)(1) of this section;" "to review and comment on findings and proposals developed by other organizations and agencies and to make recommendations for their adoption or implementation by local, State, national, or international agencies;" and "to issue an annual report on the state of the Nation's health, its health services, their costs and distributions, and to make proposals for improvement of the Nation's health statistics and health information systems").

117. 15 U.S.C. § 6801 (2012).

> Exchange Commission, and the Federal Trade Commission shall each prescribe, after consultation as appropriate with representatives of State insurance authorities designated by the National Association of Insurance Commissioners, such regulations as may be necessary to carry out the purposes of this subchapter with respect to the financial institutions subject to their jurisdiction under section 6805 of this title.
>
> (2) Coordination, consistency, and comparability
>
> Each of the agencies and authorities required under paragraph (1) to prescribe regulations shall consult and coordinate with the other such agencies and authorities for the purposes of assuring, to the extent possible, that the regulations prescribed by each such agency and authority are consistent and comparable with the regulations prescribed by the other such agencies and authorities.[118]

While this text does not explicitly require the involvement of private industry groups, in practice the financial institutions regulated by each of the above entities and the state insurance authorities work closely with these regulators, particularly with respect to the promulgation of new regulations.[119] Furthermore, as alluded to above, the core competency of these agencies (especially at the time of GLBA's enactment) was not information security. Financial institutions, by contrast, had substantial incentive to invest in information security, a fact revealed by the CISO interviews[120] and supported by the quantitative analysis below.[121] As such, it seems reasonable to expect that, although not explicitly mandated by Congress, these agencies would actively seek the involvement of industry stakeholders in a manner more similar to that required for

118. 15 U.S.C. § 6804(a)(1–2) (1999) (updated with some differences in language in 2011).
119. Thaw, *supra* note 55, at 29.
120. *See* discussion *infra* Part IV.
121. *See* discussion *infra* Part III.

HIPAA than that conducted with ordinary notice-and-comment procedures under the APA.

In essence, we see in this final category a form of informal rulemaking employing "Notice-and-Comment-Plus-Plus," where not only do the organic statutes require the administrative agencies to engage more than the baseline requirements of § 553 of the APA, but those statutes specifically encode regulatory capture of industry stakeholders into the rulemaking process itself.

II. APPLYING THE MODEL TO INFORMATION SECURITY

The primary goal of this work is to develop a better understanding of how information security regulations function and suggest ways to improve security outcomes through regulation. The empirical approaches discussed in Parts III and IV require that existing laws and regulations be sufficiently grouped for the purposes of comparison. Based on the theoretical framework developed in Part I,[122] this Part proposes grouping the most predominant existing information security laws and regulations into two groups for the purposes of analysis: (1) Directive Regulation;[123] and (2) Management-Based Regulatory Delegation.[124]

A. Directive Regulation

Directive Regulation comprises laws and/or regulations laying out express performance standards and/or means of achieving performance. This category of regulation is directive in nature,

122. This Part discusses, but does not rely upon, the timing component of each regulation in developing the two regulatory groupings for empirical comparison. The nature of timing is such that coupling it to the form of regulation may fail to consider more precise distinctions among information security regulations. As of the time of this writing, while such precise distinctions do exist, there are an insufficient number of regulatory models in place to allow empirically valid comparison among all different models. If the trend of increasing regulation of information security practices continues, future data may be sufficient to create more fine-grained comparisons among regulatory categories. In another work, I propose a comprehensive model for such fine-grained categorization. *See* Thaw, *supra* note 55.

123. *See* discussion *infra* Part II.A.

124. *See* discussion *infra* Part II.B.

traditionally is handled by legislatures (perhaps with limited, precise delegation to administrative agencies),[125] and generally involves the specification either of means of performance or means of achievement. In the context of information security, the various state Security Breach Notification (SBN) laws are the predominant example of this form of regulation.

SBN statutes are laws requiring an entity that loses control of "personal information" it maintains about individuals to disclose that loss to those individuals.[126] As of May 2013, forty-six states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands had such laws.[127] The original intent of these laws was to help consumers protect themselves against identity theft by requiring data custodians to notify individuals when a custodian lost control of information that could facilitate identity theft.[128] SBNs generally specify what constitutes covered information, what are triggering events, who must be notified of breaches, and under what exceptions notification is unnecessary or may be delayed.[129] Each jurisdiction's SBN provides an exception to reporting requirements under which—if the data was encrypted—the entity need not report the event.[130]

To date, no state's SBN statute involves a rulemaking process by an administrative agency.[131] Rather, the text of the statute fully specifies all aspects of the notification requirements and exemptions.[132] In this regard, SBNs are directive legislation.

---

125. To the extent agencies promulgate regulations strictly to enforce specific legislative mandates and without substantial exercise of agency discretion, such regulations may also fall into this category. As of the time of writing, the author is unaware of any such examples of this model in the information security regulatory context.

126. *State Security Breach Notification Laws*, *supra* note 41.

127. *Id.*

128. *See, e.g.*, CAL. ASSEMB., CAL. BILL ANALYSIS, S.B. 1386, 2001–02 Reg. Sess. (2002) (Senate Third Reading and analysis of Saskia Kim).

129. *See, e.g.*, O.C.G.A. §§ 10-1-910 to -912 (West 2007). For a list of all states with Security Breach Notification laws, see *State Security Breach Notification Laws*, *supra* note 41.

130. § 912.

131. The Massachusetts Data Security Standards do involve an administrative agency, but not as respects the details of the breach notification requirement. These aspects are fully captured in the text of the law passed by the General Court of the Commonwealth of Massachusetts. MASS. GEN. LAWS ch. 93H, § 2 (2013).

132. Massachusetts's statute does define the meaning of "encrypted" in its statutory text. MASS. GEN.

On their face, SBNs appear to be traditional performance-based regulations targeting the Output/Efficacy Stage of the ISPL. The aspect of SBNs relating to the condition they seek to prevent is best characterized as performance-based regulation. It specifies a condition—the loss of control of personal information—which is undesirable and should be avoided. That condition is an outcome—whether or not the "security" of a system has been breached[133]—and is clearly measured at the Output/Efficacy Stage of the ISPL.

Consider, for example, the following language from New York State's SBN:

> Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information[134] shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the

---

LAWS ch. 93H, § 1(a). It is worth noting that Massachusetts's statute, unlike most other states' SBNs, does *permit* the Department of Consumer Affairs and Business Regulations to adopt regulations to revise the definition of "encrypted." MASS. GEN. LAWS ch. 93H, § 1(b). However, it neither *requires* the Department do so, nor does it appear that if the Department were to do so, that it would have anything more than a marginal impact on the applicability of the statute.

133. "Breach" in this context refers to any compromise of administrative, technical, or physical procedures resulting in the acquisition of information by an unauthorized party.

134. N.Y. GEN. BUS. LAW § 899-aa(1)(b) (McKinney 2013) ("'Private information' shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: (1) social security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account."). For the definition of "personal information," see § 899-aa(1)(a) ("'Personal information' shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.").

breach and restore the reasonable integrity of the system.[135]

This statute essentially requires disclosure when any of an individual's social security number, driver's license/non-driver identification number, or financial account number *in connection with* information that identifies that individual (e.g., their name) is acquired by an unauthorized person as the result of a data breach.[136]

The focus here is on the "breach in the security of the system" language that is used several times throughout the statute. This language is the "triggering event" that results in the "penalty" aspect of the regulation—requirements to notify individuals.[137] Thus this aspect of New York State's SBN is best described as an "output" or as relating to the effectiveness of the system, and thus is best considered as part of the Output/Efficacy stage. Because the text of the statute explicitly identifies this condition, it is best described as targeting that condition, rather than generating an effect. The other U.S. jurisdictions that have such laws use statutory language producing an effect similar to that defined above.[138] SBNs, therefore, have the characteristic of being performance-based regulation targeting the Output/Efficacy Stage of the production lifecycle.

It is also important to note that a primary impetus behind the passing of California Senate Bill 1386, which later became what is now California's SBN, was the desire to improve the ability of "[California] consumers [to] protect their financial security."[139] Specifically, the legislature sought to accomplish this by establishing

135. N.Y. GEN. BUS. LAW § 899-aa(2).

136. *Id.* § 899-aa.

137. New York State also has a centralized notification requirement (§ 899-aa(8)(a)) which requires notification of three state agencies in the event of any breach affecting New York State residents and a consumer reporting agency notification requirement (§ 899-aa(8)(b)) which requires notification of the three major consumer reporting agencies in the event of a breach affecting more than 5,000 New York State residents. *Id.* § 899-aa(8)(a)-(b).

138. *See, e.g.*, CAL. CIV. CODE §§ 1798.81.5–1798.82 (West 2006); CONN. GEN. STAT. § 36(a)-701 (2006). *See also State Security Breach Notification Laws*, *supra* note 41 (providing a current listing of and citations to all U.S. jurisdictions with SBNs).

139. CAL. ASSEMB., CAL. BILL ANALYSIS, S.B. 1386, 2001–02 Reg. Sess. (2002) (Senate Third Reading and analysis of Saskia Kim).

law requiring organizations to make consumers aware of when their data was compromised.[140] This impetus does not affect the present analysis of the law's character, as it simply defines the social goal that the performance-based means were chosen to advance.[141] The impetus is, however, important to note, and it raises the question of whether the law is actually effective at achieving this goal.

Interviews with CISOs revealed the surprising result that SBNs had a predominant effect of driving the implementation of technical practices.[142] Specifically, organizations began to institute unilateral laptop/portable media encryption policies.[143] According to several respondents, this effort was not a response to any particular evidence that doing so would decrease the number of individuals whose identity was stolen as a result of data breaches,[144] but rather in response to the spread of SBNs throughout U.S. jurisdictions and the high-profile security incidents disclosed pursuant to those laws. Consider, for example, the following excerpts from one interview with the CISO of a large healthcare organization:

> And so what's been really interesting about the notification laws is [they] have come in and they have essentially reversed the whole direction security was taking . . . the security investment is moved essentially to crypto. Just encrypt as much as you can. Whatever it takes, just encrypt it. If it moves, encrypt it. If it stays there, encrypt it.[145]

According to this respondent, SBNs have directly resulted in the respondent's organization implementing encryption policies for all of their portable computing devices and media.[146] These policies clearly

140. *Id.*
141. *Id.*
142. *See* discussion *infra* Part IV; Thaw, *supra* note 55, at 22.
143. Thaw, *supra* note 55, at 22 n.66.
144. This is not to say that doing so would not have an effect in reducing identity theft, nor is it to say that encrypting portable media is an ineffective security practice.
145. Thaw, *supra* note 55, at 37.
146. *Id.*

result in the adoption of a specific technology (encryption), a classic example of the means-based regulation parameter. The respondent also specifically describes how *existing* data and devices will be encrypted: "Just encrypt as much as you can. Whatever it takes, just encrypt it."[147] This language implies that the "reversal" in organizational direction resulted in *post-facto* changes to the existing system, thus producing an effect at the Implementation/Maintenance Stage. While one might imagine a policy change involving encryption to affect the Design/Planning Stage,[148] the language in this instance makes clear that effect occurs at the Implementation/Maintenance Stage in this respondent's organization.[149] Finally, although perhaps obvious, it is worth noting that the respondent's language describes an effect resulting from the introduction of SBNs, not the specific intent of the SBNs themselves.[150] The intended "targets" of SBNs were the reduction of data breach incidents and ensuring that individuals were made aware when their identity had been placed at risk of "theft" or other use in fraudulent activity.[151]

Another respondent identified this same effect of SBNs driving encryption, although interestingly did so in a more positive context.[152] The respondent described how it simplified their organization's process of complying with the law, and provided their organization flexibility in selecting specific technologies to meet the encryption "goal":

147. *Id.*

148. For example, a policy that an organization's security professionals must design a system capable of scanning all future (and possibly existing) data for qualifying "sensitive information" and, when such information is found, that information must automatically (via some technical mechanism) become subject to encryption requirements. An approach of this form would more substantially affect the Design/Planning stage than that policy discussed by this respondent.

149. In this sense, the encryption mandate was both a directive to do things a certain way in the future (Design/Planning stage) and a directive to layer encryption onto existing systems (Implementation/Maintenance stage).

150. Thaw, *supra* note 55, at 37–38.

151. *Id.* at 38.

152. *Id.*

> . . . despite my reservations about SB-1396, on which most of the breach notification legislation has been modeled, it was exemplary in one regard . . . it was an extremely small piece of legislation . . . [that] has the whole encryption safe harbor concept built into it which [], in practice, has turned out to be very prescient. . . . [D]espite my issues with it, there is a difference between [a] breach and a loss of custody, and [the encryption safe harbor] is a very good example of how to manage [compliance to avoid reporting].[153]

The respondent here clearly does not think that ordinary loss of custody, such as a laptop being stolen in a public café, should give rise to a reportable incident. Yet the respondent indicates, nonetheless, that the encryption safe harbor has simplified their responsibilities by providing a single method for "compliance" with SBNs (avoidance of the reporting requirement)—encrypting all portable computing devices and media.[154] The respondent further notes that they find this style of approach preferable "'[b]ecause it does not legislate technology,'" referring to the fact that their organization is able to select which encryption technologies are used to achieve the goal.[155]

While both respondents identify a condition supporting the proposition that SBNs have an effect of driving the use of encryption technology, it is interesting to note the divergent views they took as to the appropriateness of that approach. These divergent views may provide insight into the effects of this type of regulation on different types of organizations. I explore this concept further in Part IV.[156]

Interestingly, in addition to being one form of regulation considered by this work, SBNs are also the cause enabling the quantitative analysis used to compare directive regulation and Management-Based Regulatory Delegation. As discussed further in

153. *Id.*
154. *Id.*
155. *Id.*
156. *See* discussion *infra* Part IV.

Part III, the notification requirement of SBNs gives rise to sufficient security incident reporting to facilitate analysis of regulatory impact.[157] Based on the data available, it seems unlikely a sufficient number of incidents would have been reported without these laws to allow statistically-valid analysis.

B. Management-Based Regulatory Delegation

Management-Based Regulatory Delegation is a mode of regulation under which administrative agencies, through legislative-mandated collaboration with regulatory stakeholders, promulgate regulations requiring regulated entities to develop plans designed to achieve certain aspirational goals laid out by the legislature. The regulatory goal in this case is the development of the compliance plan itself (and possible adherence to that plan), rather than the necessary achievement of stated goals or usage of certain means to achieve those goals, as is the case with directive regulation.

This category of regulation is a combination of two threads of discussion in the current literature: 1) Coglianese and Lazer's management-based regulation;[158] and 2) Bamberger's regulatory delegation.[159] Management-based regulation relies on a concept of administrative agencies promulgating requirements that regulated entities develop (and possibly adhere to) compliance plans.[160] The application of this paradigm, once decoupled from issues of timing, to information security regulation is relatively straightforward. It is, however, incomplete for two reasons. First, Coglianese and Lazer's conception fails to capture the concept of legislatively-mandated involvement of private parties (regulatory capture). Second,

157. *See* discussion *infra* Part III.

158. Coglianese & Lazer, *supra* note 24.

159. Bamberger, *supra* note 18, at 385; Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 265–70 (2011) [hereinafter Bamberger & Mulligan, *Privacy on the Books*] (discussing the limited reach of privacy regulation in shaping privacy practices); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 79-80 (2008) [hereinafter Bamberger & Mulligan, *Privacy Decisionmaking*], *available at* http://ssrn.com/abstract=1104728.

160. Coglianese & Lazer, *supra* note 24, at 692.

management-based regulation alone fails to capture the degree to which organizations may be subject to other incentives not directly enshrined in but resulting from the structure of the regulation.

As Bamberger (and later Bamberger and Mulligan) discuss,[161] in certain contexts regulators lack the experience or resources necessary to understand and/or keep pace with the myriad different challenges facing regulated entities (particularly in heterogeneous industries[162])[163] or to promulgate regulations lacking relevance to guide business decision-makers (particularly in privacy matters).[164] The result is a circumstance in which, to move forward effectively, regulators must rely increasingly on input from regulated entities. Management-based regulation provides a solid foundation for such an approach but requires greater input from stakeholders than envisioned by Coglianese and Lazer to ensure the promulgated regulations setting forth compliance plan requirements are sufficiently robust to avoid a compliance "race to the bottom."[165] This is particularly true in the context of information security, where regulators rely heavily on a concept of "reasonableness"—a concept traditionally understood in law, but lacking operational meaning in the context of information security due to a lack of an appropriate "reasonable person" standard[166] and a lack of a well-agreed upon *licensed* professional standard upon which to rely for expert advice.[167]

---

161. *See generally* Bamberger, *supra* note 18; Bamberger & Mulligan, *Privacy on the Books*, *supra* note 159; Bamberger & Mulligan, *Privacy Decisionmaking*, *supra* note 159.

162. Heterogeneity among regulated entities is a particularly acute problem in the information security regulatory context since cybersecurity regulation generally targets entities whose core competency is *not* information security (or even information technology). The vast majority of organizations custodian to sensitive information regulated by the laws discussed here are in the healthcare or finance sectors, as well as other entities across all industrial sectors who handle substantial volumes of consumer records. *See* discussion *infra* Part IV.

163. Bamberger, *supra* note 18, at 387.

164. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 159, at 266.

165. Coglianese and Lazer *supra* note 24, 700–02; Thaw, *supra* note 55, at 30–31.

166. The "reasonable" layperson likely lacks any meaningful understanding of information security practices and certainly is incapable of evaluating those practices.

167. Many professional "certifications" exist, most notably the Certified Information Systems Security Professional (CISSP) certification, administered by the International Information System Security Certification Consortium ($(ISC)^2$). However, to-date these certifications remain largely

By extending the concept of management-based regulation to include a concept of regulatory delegation to private entities (particularly with substantial involvement of private parties in the rulemaking process, as described above), the model proposed here addresses the concomitant challenges of a rapidly evolving regulatory climate, substantial heterogeneity among regulated entities, and a need for sufficiently well-defined regulations so as to avoid a regulatory "race to the bottom" in an environment relying heavily upon but lacking a good definition of "reasonableness."[168]

Thus, merging the concepts of management-based regulation and regulatory delegation provides a category into which to group information security laws and regulations for the purposes of comparison. The sections that follow examine this combination of principles in the context of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[169] the Gramm-Leach-Bliley Financial Modernization Act (GLBA),[170] and the regulatory jurisprudence of the Federal Trade Commission (FTC)[171] through its enforcement actions and consent decrees on information security matters. The combination of these two themes in regulation allows these three core areas of information security regulation to be understood together. Understanding them together is important because of the degree to which their evolution relied upon one another and as a result the degree to which they share common characteristics as a class of regulation.

---

vocational training certificates and do not equate to the standard of "learned professionals" the law often turns to in complex areas such as science, medicine, and engineering where a "reasonable person" standard cannot be adopted from the average layperson. *See generally Certified Information Systems Security Professional*, $(ISC)^2$, https://www.isc2.org/cissp/default.aspxhttps://www.isc2.org/ (last visited Jan. 22, 2014).

168. Curiously, this merger of the need for flexibility as to response with a lack of definition as to compliant appears to parallel the traditional philosophical quandary of concurrently needing both structure and flexibility. It may be worth exploring further to determine under what other circumstances (i.e., what other regulatory contexts) this set of circumstances may arise and whether the blended regulation solution proposed herein may be applicable.

169. *See infra* Part II.1.

170. *See infra* Part II.2.

171. *See infra* Part II.3.

1. Health Insurance Portability and Accountability Act Security and Privacy Rules (HIPAA)

HIPAA was passed in 1996 as part of a broad effort to reform various aspects of the healthcare and health insurance systems in the United States.[172] As part of the legislation, Congress included provisions with respect to the information security of certain information describing the identity, medical conditions, and finances of individuals.[173] This information is collectively termed Protected Health Information (PHI)[174] and includes information created or received by entities involved in the healthcare process relating to the health condition or care of an individual.[175]

The provisions pertaining to information security apply to any organization which is a Covered Entity or (under certain circumstances) a Business Associate of a Covered Entity.[176] Covered Entities generally include health (insurance) plans, healthcare information clearinghouses, and healthcare providers.[177] Business Associates generally include any organization that works with a Covered Entity and handles PHI on behalf of or to provide services to the Covered Entity.[178] Although there has been some discussion as to the applicability of various aspects of the term Business Associate, these definitions generally mean that the HIPAA Security Rule applies to all healthcare insurance organizations, processing organizations that support healthcare insurance organizations, medical providers (if they use electronic records), and any other

172. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 26 U.S.C., 29 U.S.C., and 42 U.S.C.).

173. 42 U.S.C. § 1320d-2 (2006).

174. Originally the statute described this information as "Individually Identifiable Health Information." 42 U.S.C. § 1320d(6). The implementing regulations promulgated by the Department of Health and Human Services collectively termed information subject to HIPAA's Privacy and Security rules as "Protected Health Information." 45 C.F.R. § 160.103 (2013).

175. 42 U.S.C. § 1320d(6)(B).

176. 45 C.F.R. § 160.103.

177. *Id.*

178. *Id.*

entities that engage in business with them if that business transaction involves the exchange or handling of PHI.[179]

The HIPAA Security Rule comprises two key elements: (1) a statutory instruction by Congress for the Department of Health and Human Services to promulgate regulations establishing information security standards for the handling of PHI[180] and (2) a general instruction to organizations covered by the Rule that they maintain appropriate administrative, technical, and physical safeguards.[181] The first element is the key provision under which specific information security regulations part of HIPAA are promulgated. It generally requires that the regulations take into account available technologies, costs of security measures, training needs, the value of various security measures, and the varying sizes of healthcare organizations and providers.[182]

The regulations promulgated by the Secretary of Health and Human Services pursuant to this provision[183] are too numerous to list here in a comprehensive fashion, and doing so would not substantially illuminate the discussion of characterizing HIPAA's Security Rule as a regulatory device. Rather, it is worth examining the method by which the regulations are promulgated and the substantive breadth of resultant regulations in the context of the ISPL.

HIPAA is a hybrid form of management-based regulation. It exhibits the classic characteristics of management-based regulation, requiring firms to conduct risk assessments and develop plans to address the identified risks.[184] The HIPAA regulations also specify certain protection measures that regulated organizations must undertake, similar to means-based regulation.[185] Unlike traditional means-based regulation, however, the regulations do not specify the

179. *Id.*
180. 42 U.S.C. § 1320d-2(d)(1) (2006).
181. *Id.* § 1320d-2(d)(2).
182. *Id.* § 1320d-2(d).
183. 45 C.F.R. §§ 164.102–.534 (2013).
184. 42 U.S.C. § 1320d-2(d)(2).
185. *Id.*

implementation details for those measures. Rather, such regulations explicitly leave those implementation details to the regulated entities.[186]

HIPAA involves a notice-and-comment process with legislative direction to give deference to key stakeholders.[187] Specifically, it requires the Department of Health and Human Services to consult with the National Committee on Vital and Health Statistics, which comprises key stakeholders from industry, government, and academia.[188]

The regulations promulgated under the HIPAA Security Rule bear many aspects of traditional management-based regulation under Coglianese and Lazer's typology. The general requirements[189] and flexibility of approach[190] specified in the general rules for security standards require organizations to ensure the confidentiality, integrity, and availability of electronic medical records, protect against reasonably anticipated threats, and ensure workforce compliance.[191]

This general requirement that organizations engage in comprehensive activities to protect their information assets typifies management-based regulation. The "flexibility of approach" provision effectively delegates the responsibility for planning these activities to the regulated entity, thereby exhibiting the classic form of management-based regulation. This provision provides that covered entities may use any security measures reasonably and appropriately capable of achieving the specific security goals and requires that the entity take into account its size, scope, complexity, current technical infrastructure, costs, and levels of risk in making such determinations as to reasonableness.[192]

186. *Id.*
187. 42 U.S.C. § 1320d-2(a)(5).
188. *Id.* § 1320d-2(a)(5)(B).
189. 45 C.F.R. § 164.306(a) (2013).
190. *Id.* § 164.306(b).
191. *Id.* § 164.306(a)–(b).
192. *Id.* § 164.306(b).

Furthermore, in addition to this flexibility of approach, the regulations specifically require regulated entities to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity . . . ."[193] and to "[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)."[194] These directives to conduct risk assessments and implement security measures consistent with those risk assessments are perfect examples of traditional management-based regulation.

The HIPAA Security Rule is far more expansive, however, than the assessment and planning requirements outlined above. Unlike traditional management-based regulation, it goes on to detail highly-specific elements the plan must contain—almost taking it to the degree of means-based regulation, but stopping short by leaving the details of implementation to the discretion of the regulated entity consistent with the flexibility of approach provisions outlined above.[195] Consider the following four provisions of the HIPAA Security Rule regulations:

> (i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.
> (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
> (iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
> (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health

193. 45 C.F.R. § 164.308(a)(1)(ii)(A) (2013).
194. *Id.* § 164.308(a)(1)(ii)(B).
195. *Id.* § 164.306(b).

information.[196]

The four provisions are the "implementation specifications" for the "standard" specified in 45 C.F.R. § 164.312(a)(2) governing access control, which states that regulated organizations must "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)."[197] The standard clearly resembles management-based regulation, but the implementation specifications diverge from traditional management-based regulation by clearly targeting the Implementation/Maintenance Stage of the ISPL.[198] This bifurcated approach is replicated in nearly all sections of the regulations implementing the HIPAA Security Rule, thus suggesting that HIPAA is also management-based regulation that targets the Implementation/Maintenance Stage of the ISPL.[199] As discussed in Part IV, this bifurcation has implications for the relationship between senior managers and information security professionals at regulated organizations.[200]

2. Gramm-Leach-Bliley Financial Modernization Act (GLBA)

The Gramm-Leach-Bliley Financial Modernization Act of 1999[201] specifies requirements for the Financial Institutions Safeguards Rule (Safeguards).[202] The Safeguards require that certain federal financial regulators promulgate regulations establishing standards for

196. 45 C.F.R. § 164.312(a)(2) (2013).
197. *Id.* § 164.312(a)(1).
198. Thaw, *supra* note 55, at 43.
199. *Id.*
200. *See* discussion *infra* Part IV.
201. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., 16 U.S.C., 18 U.S.C., and 29 U.S.C.).
202. 15 U.S.C. § 6801(b) (2012).

administrative, technical, and physical safeguards against information security threats to consumer financial data.[203]

The Safeguards require each of the agencies[204] charged with enforcing the provisions of GLBA to promulgate regulations implementing the Rule.[205] The FTC has promulgated a series of regulations pursuant to the Safeguards, which they call the "Safeguards Rule."[206] The OCC, the Federal Reserve, the FDIC, and the OTS jointly issued regulations, which they call the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Consumer Notice" ("Interagency Guidelines").[207] I examine each of these two sets of regulations to illustrate that GLBA, like HIPAA, is also a form of bifurcated management-based regulation targeting both the Design/Planning Stage of the ISPL and the Implementation/Maintenance Stage of the ISPL. Collectively these cover all organizations included in the CISO interviews.[208] Based on those interviews, the author's experience in private practice, and discussions with practitioners, these rules

203. *Id*.

204. At the time of its enactment, GLBA charged seven federal regulatory agencies with enforcing the privacy and security provisions of the Act, specifically including promulgating regulations to implement these provisions of GLBA. These agencies included: (1) the Office of the Comptroller of the Currency (OCC); (2) the Board of Governors of the Federal Reserve Systems (Federal Reserve); (3) the Federal Deposit Insurance Corporation (FDIC); (4) the Office of Thrift Supervision (OTS); (5) the Board of the National Credit Union Administration (NCUA); (6) the Securities and Exchange Commission (SEC); and (7) the Federal Trade Commission (FTC). 15 U.S.C. §§ 6805(a), 6809(2) (2012). Section 6805(a)(6) technically permits state insurance regulators to engage in enforcement of the GLBA Safeguards Rule, however considering the actions of state regulators in this regard is outside the scope of analysis for this paper. It is unclear why the Commodity Futures Trading Commission (CFTC), which has other regulatory roles under GLBA, was not explicitly listed in Section 6805(a). This is particularly interesting considering the CFTC recently promulgated regulations pursuant to the GLBA Privacy rule. Joshua Lynch, *CFTC Proposes Rules on Affiliate Marketing, Data Disposal, and GLBA Privacy*, CHRON. DATA PROTECTION, http://www.hldataprotection.com/2010/10/articles/financial-privacy/cftc-proposes-rules-on-affiliate-marketing-data-disposal-and-glba-privacy/ (last visited Jan. 22, 2014).

205. 15 U.S.C. § 6801(b).

206. 16 C.F.R. § 314 (2013).

207. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736-01 (Mar. 29, 2005) (codified at scattered sections of 12 C.F.R. pt. 30).

208. *See* discussion *infra* Part IV.

comprise the bulk of financial regulatory rules driving information security compliance.[209]

GLBA has some aspects that suggest Congress intended to involve industry in the notice-and-comment rulemaking process. Additionally, as discussed in Part IV, the CISO interviews revealed that financial institutions had substantial incentive to participate in this process.[210] While not as stark an example as HIPAA, it appears that Congress's intent with respect to GLBA was more oriented toward a regulatory delegation model than toward the traditional notice-and-comment process.[211]

a. The FTC GLBA "Safeguards Rule"

The FTC regulations are particularly notable because, as discussed in Part II, the Safeguards Rule guided certain key elements of the FTC's jurisprudence in their privacy and data security enforcement actions.[212] The implementing regulations promulgated by the FTC specify that regulated entities must develop, implement, and maintain comprehensive written information security programs addressing administrative, technical, and physical risks to the security and confidentiality of customer information.[213]

These regulations are a classic example of management-based regulation. They require individual-regulated organizations to develop plans appropriate to each organization's size, scope, and complexity to achieve a set of specified objectives related to information security. The objectives are described in broad categories, directing the organization but leaving wide discretion to innovate in selecting approaches for compliance. This is precisely

209. Not discussed in this work are the information security guidelines promulgated by the Internal Revenue Service. These guidelines generally apply to few entities and, as yet, there is no evidence they drive compliance effects on a significant scale.

210. *See* discussion *infra* Part IV.

211. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, § 5136A(a)(5), 113 Stat. 1338, 1374 (1999) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., 16 U.S.C., 18 U.S.C., and 29 U.S.C.).

212. 16 C.F.R. § 314.2(c) (2013).

213. *Id.*

consistent with the concept of management-based regulation discussed above.

The FTC's GLBA Safeguards Rule goes on to provide some limited additional specification as to what each information security program shall contain, requiring that "[i]n order to develop, implement, and maintain [an] information security program, [regulated organizations] shall" engage in a specified series of activities to design and maintain that plan.[214] These generally include designation of specific employee(s) with responsibility for the plan, identification of reasonably foreseeable security risks, development of controls and procedures to mitigate those risks, oversight of service providers to ensure their activities are consistent with the plan, and periodic evaluation and revision of the information security plan.[215]

These specifications are not so overly detailed with respect to implementation so as to suggest a means-based character of regulation, nor do they sufficiently interfere in that regard so as to suggest targeting of the Implementation/Maintenance Stage. The FTC's guidelines, however, do have an interesting requirement of regulated organizations to "regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems and procedures"[216] and "[e]valuat[ing] and adjust[ing] [the] information security program in light of the results of [that testing]."[217] This regular testing and evaluation requirement speaks directly to outcomes and, in this regard, targets the Output/Efficacy Stage of the ISPL. This is reinforced by the evaluation and adjustment requirement which, while effectively requiring the organization to repeat the risk assessment process at regular intervals, ties the conduct of those repeated assessments to the outcomes sufficiently to

214. *Id.* § 314.4.
215. *Id.*
216. *Id.* § 314.4(c).
217. *Id.* § 314.4(e).

suggest that the Output/Efficacy Stage is substantially targeted by this regulation.[218]

b. The GLBA Interagency Guidelines on Information Security

The GLBA Interagency Guidelines on Information Security differ from the FTC's GLBA Safeguards Rule in that they are a form of bifurcated management-based regulation that targets both the Design/Planning and Implementation/Maintenance Stages of the ISPL. The bifurcation present in the Interagency Guidelines is structurally very similar to that present in HIPAA.

The Interagency Guidelines begin with a general directive specifying that each organization shall design and implement a written information security plan, addressing administrative, technical, and physical safeguards and considering the nature and scope of the regulated entity, designed to ensure the security and confidentiality of customer information and protecting against threats to that information.[219] Interestingly, unlike some other general directives, this one also includes a specific reference to data disposal requirements.[220]

Just as with the FTC's GLBA Safeguards Rule above, these regulations represent a classic example of management-based regulation. They require individual regulated organizations to develop plans appropriate to each organization's size, scope, and complexity to achieve a set of specified objectives related to information security.[221] The objectives are described in broad categories, directing the organization but leaving it wide discretion to innovate in selecting approaches for compliance.[222]

Like the HIPAA regulations discussed above, the Interagency Guidelines also specify in detail what elements an information

218. Thaw, *supra* note 55, at 46.
219. 12 C.F.R. § 30, App. B § (II) (2013).
220. *Id*. § (II)(B)(4).
221. *Id.* § (II)(A).
222. *Id.*

security program must contain and what goals those elements much achieve.[223] Generally, they include requirements for access controls, encryption, administrative procedures, segregation of duties, employee background checks, system monitoring (specifically including intrusion detection), incident response, training, and regular testing of systems.[224]

The Interagency Guidelines lack the details as to implementation, however, that would qualify a means-based classification of their regulatory style. Nonetheless, the degree of detail as to areas that must be covered substantially interferes at the Implementation/Maintenance Stage so as to conclude that these regulations are a form of management-based regulation that targets the Implementation/Maintenance Stage of the ISPL. Interestingly, unlike the FTC's GLBA Safeguards Rules, the Interagency Guidelines lack the ongoing re-evaluation requirement that targets the Output/Efficacy Stage of the ISPL.[225]

3. FTC Enforcement Action/Jurisprudence

Beginning in the early 2000s, the Federal Trade Commission conducted investigations into and brought enforcement actions against organizations that exhibited poor information security practices in the handling of personal information, sensitive information, or both.[226] Their primary statutory basis[227] for doing so

223. *Id.* § (III)(A–B).

224. *Id.* § (III)(C).

225. *Compare* 16 C.F.R. § 314.4(e) (2013) (GLBA Safeguards), *with* 12 C.F.R. § 30, App. B (Interagency Guidelines).

226. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 144 COLUM. L. REV. (forthcoming 2014); Christopher Wolf, *Enforcement and Policy at the FTC and the Impact on Businesses*, BrightTALK (Apr. 8, 2010), https://www.brighttalk.com/webcast/288/20491.

227. There are a number of other secondary statutory bases upon which the FTC rests its data security enforcement actions, including the Fair Credit Reporting Act (15 U.S.C. §§ 1681–81u), the Fair and Accurate Credit Transactions Act of 2003 (FACTA) (15 U.S.C. §§ 1681–81x), the Health Information Technology for Economic and Clinical Health Act (Pub. L. No. 111-5, 123 Stat. 226 (codified in scattered parts of 42 U.S.C.)), the Gramm-Leach-Bliley Financial Modernization Act (discussed above in Part II.2), and the Children's Online Privacy Protection Act (15 U.S.C. §§ 6501–05). For the purposes of this section, with the exception of GLBA, these secondary bases are unimportant as to the classification of the FTC's jurisprudence according to my revised typology of information security

was Section 5 of the FTC Act, which grants the Commission the authority to investigate and challenge business practices it finds unfair or deceptive.[228] Pursuant to this authority, the FTC brought several enforcement actions[229] against organizations it believed to have engaged in "unfair or deceptive" information security practices that violate Section 5.[230] Generally speaking, the Commission asserted as "deceptive" those practices where organizations promised one level of security and failed to deliver that level of security,[231] and asserted as "unfair" those practices where organizations failed to provide a reasonable and appropriate level of security in protecting sensitive and/or personal information.[232]

In practice, nearly all these matters result in a settlement between the organization under investigation and the Commission.[233] These settlements generally include the following elements: (1) an agreement to discontinue, correct the offending information security practices; or both,[234] and (2) an agreement to engage in ongoing periodic information security assessments the results of which must be attested to by a certified professional.[235] In rare circumstances where the violation alleged is so severe and the resultant consumer

---

regulation.

228. 15 U.S.C. § 45(a) (2006).

229. In a few notable cases where the Commission deemed it appropriate, in conjunction with the Department of Justice, the FTC brought actions in federal district court rather than as an enforcement action. The effective result was the same, with those matters reaching settlement under the jurisdiction of the court rather than a consent decree under the jurisdiction of the Commission. *See, e.g.*, Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief, United States v. Choicepoint, Inc., No. 06-CV-0198 (N.D. Ga. Jan. 30, 2006), 2006 WL 236338; Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief, United States v. Choicepoint, Inc., No. 06-CV-0198 (N.D. Ga. Feb. 15, 2006), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf (regarding the form of settlement).

230. *See, e.g.*, *In re* Twitter, Inc., No. C-4316, 2011 WL 914034 (F.T.C. Mar. 2, 2011); *In re* Microsoft Corp., 134 F.T.C. 709 (2002).

231. *Twitter, Inc.*, 2011 WL 914034, at *4; *Microsoft Corp.*, 134 F.T.C. 709, 748-50.

232. *In re* TJX Cos., No. C-4227, 2008 WL 3150421, at *2 (F.T.C. July 29, 2008); *In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 WL 2395788, at *2 (F.T.C. Sept. 20, 2005).

233. *See, e.g.*, *BJ's Wholesale Club, Inc.*, 2005 WL 2395788, at *2.

234. *See, e.g.*, *In re* DSW Inc., File No. 052-3096, 2005 WL 3366974, at *4 (F.T.C. Dec. 1, 2005) (requiring DSW to implement a "comprehensive information security program").

235. *See, e.g.*, *DSW Inc.*, 2005 WL 3366974, at *4–5 (explaining that certain *certified* (as opposed to licensed) professional(s) are eligible to certify these assessments).

harm alleged so grievous, the Commission may also require compensatory or punitive damages.[236] These consent decrees and settlements form the basis for the aspects of FTC data security enforcement used herein to classify the regulatory style of the Commission's jurisprudence. Generally, the FTC's style of regulation is a mix between management-based regulation and means-based regulation targeting all stages of the ISPL.

The initial and ongoing risk assessment requirement of the FTC's GLBA Safeguards Rule is best described as a bifurcated style of management-based regulation that targets both the Design/Planning and the Efficacy/Output Stages of the ISPL. This is perhaps unsurprising, given that the Commission identified in a 2005 prepared statement to Congress that it based its risk assessment requirements in its enforcement action consent decrees upon those requirements in the Safeguards Rule:

> To date, the Commission has brought five cases against companies for deceptive security claims, alleging that the companies made explicit or implicit promises to take reasonable steps to protect sensitive consumer information. Because they allegedly failed to take such steps, their claims were deceptive. The consent orders settling these cases have required the companies to implement rigorous information security programs generally conforming to the standards set forth in the GLBA Safeguards Rule.[237]

Like the risk assessment requirements in HIPAA and GLBA, the risk assessment requirements under the FTC's enforcement action settlements require organizations to engage in an initial risk assessment within a specified period of time, develop an information

236. 15 U.S.C. § 45(l) (1994) (stating that such matters often end up in federal district court).

237. *Enhancing Data Security: The Regulators' Perspective: Hearing Before theSubcomm. on Fin. Inst. & Consumer Credit of the H. Comm. on Fin. Servs.*, 109th Cong. 14 (2005) (prepared statement of the Federal Trade Commission delivered by Lydia Parnes, Director of the Bureau of Consumer Protection of the Federal Trade Commission) (citations omitted).

security plan consistent with that risk assessment, conduct periodic assessments thereafter, and update their information security plans accordingly.[238]

The provisions pertaining to the conduct of an initial risk assessment and development of an initial information security program are classic examples of a management-based style of regulation, with the slight exception that they are the result of an enforcement action by an administrative agency and apply to a specific organization rather than the result of rules promulgated by an administrative agency and applicable to all regulated entities thereunder. However, this difference does not change the functional character of the regulation. The provisions detailing what substantive areas the assessment and plan must cover are sufficiently broad so as neither to implicate a functional character of means-based regulation nor to interfere substantially at the Implementation/Maintenance Stage of the ISPL. The intent of the regulation clearly is targeted because the requirements are the result of an enforcement action against a specific organization. Thus the classification of the regulation in this regard is management-based regulation targeting the Design/Planning Stage of the ISPL.

The FTC's settlements also include requirements for ongoing risk assessments and updating of the information security program as appropriate based on the results of those ongoing assessments.[239] This regular assessment requirement speaks directly to information security outcomes and, therefore, targets the Output/Efficacy Stage of the ISPL. This intent characterization is reinforced by the updating requirement, which sufficiently ties the conduct of the periodic assessments to the outcomes to suggest that the Output/Efficacy Stage is substantially targeted by this regulation. Thus, the classification of the regulation in this regard is management-based regulation targeting the Output/Efficacy Stage of the ISPL. Therefore, similar to the FTC's GLBA Safeguards Rule, the FTC's

238. *BJ's Wholesale Club, Inc.*, 2005 WL 2395788, at *2.
239. *Id.*

enforcement actions—as they pertain to the subjects of the enforcement—are management-based regulation targeting each of the Design/Planning Stage and the Implementation/Maintenance Stage of the ISPL.

a. Indirect Consequences of FTC Enforcement Actions[240]

The FTC enforcement actions and settlements contain provisions identifying the offending practices as "unfair" or "deceptive" and require the subject of the enforcement action to discontinue the offending practices.[241] This is a classic form of means-based regulation, whereby the subject of the enforcement action is required to discontinue use of a specific practice, procedure, or technology.

Consider the case involving Reed Elsevier, Inc. and Seisint, Inc.[242] In this enforcement action, the FTC alleged that Reed Elsevier and Seisint (which was subsequently acquired by Reed Elsevier) failed to utilize sufficient authentication procedures with respect to verifying the identity and authorization of users of its consumer information services.[243] The FTC alleged that verified incidents of identity theft resulted from these failures.[244]

In this part of the complaint, the Commission effectively created a list of specific requirements that any comprehensive information security program satisfying the requirements of the consent decree would be required to implement.[245] By effectively requiring the

240. This section provides a (perhaps digressive) discussion of aspects of FTC enforcement that are not exactly Management-Based Regulatory Delegation. These aspects, or rather the *effects* of these aspects, are intertwined with the primary management-based aspects of the regulation. They are notable as matters of discussion in the context of this work because, as noted at the end of this section, they are consistent with and foreshadow recommendations that flow from the quantitative analysis presented. *See* discussion *infra* Part III.

241. *See, e.g.*, *In re* Reed Elsevier, Inc. & Seisint, Inc., File No. C-4226, 2008 WL 3150420 (F.T.C. July 29, 2008).

242. *Id.*

243. *Id.* at *1–2.

244. *Id.* at *3.

245. *Id.* at *7 ("Each Assessment shall: A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period; B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about

respondent organization to address these specific technical measures, the FTC engaged in a form of means-based regulation. The regulation obviously targeted the specific respondent. While some of the items identified above would require design and planning changes to resolve, the *post-facto* nature of this regulation—by the function of it being an enforcement action, not a proactive set of promulgated regulations—suggests it is more appropriately characterized as targeting the Implementation/Maintenance Stage as it will affect systems already in use by the respondent. Thus, this aspect of FTC enforcement is best classified as means-based regulation targeting the Implementation/Maintenance Stage of the ISPL.

The identification of alleged unfair or deceptive information security practices by the FTC in its various complaints has created a curious effect in how those involved in information security practice perceive the regulatory requirements to which they are subject. In short, the specific practices identified by the Commission in its complaints have resulted in rules that organizations must follow—specifically, organizations must *not* engage in those practices identified in the complaints as unfair or deceptive.

This is a curious effect, because notwithstanding the analysis above, no formal statute or regulation actually *requires* organizations (other than the subjects of the enforcement actions) to avoid such practices. There is only the threat of future enforcement by the FTC that drives such "compliance." From the practitioner's perspective, this may be an overly fine distinction. If a client asks whether an activity is permissible under federal law, and the Commission has identified it as potentially violative of Section 5 of the FTC Act, the practical answer to the client is almost assuredly to avoid the allegedly offending practice. Consider, for example, the reply of one CISO of a large information technology company who described the

consumers; C. explain how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.").

TJX enforcement action as providing some definable guidance as to what *not* to do:

> . . . so there are some don't do mechanisms that we apply by process that are also helped by regulation because if we didn't have that [regulation] to test to we might not think about it today. We couldn't get to it [that information security practice]. It wouldn't be like, 'Oh, gosh, the TJ Maxx incident is pretty good.'"[246]

This respondent identifies the TJ Maxx incident as supporting their efforts to advance certain (desirable) information security practices and suggests that absent the FTC's enforcement action in response to the incident, they might not be able to defend those practices within their organization.[247]

Collectively, the discussion above identifies ways in which FTC enforcement actions result in *de facto* regulations affecting each stage of the ISPL. While the empirical evidence in this regard is preliminary, it is consistent with the conclusions from the quantitative comparisons presented in Part III.[248]

III. QUANTITATIVE COMPARISONS: TRACKING SECURITY BREACH INCIDENCE

In many areas of regulation, such as pollution control and food safety, quantitative measures provide critical insight into regulatory efficacy. Information security poses a somewhat more difficult challenge in this regard, because it—by definition—lacks a control population against which to test effectiveness of security measures.[249]

246. Thaw, *supra* note 55, at 54.

247. *Id.*

248. *See* discussion *infra* Part III.

249. This is because it is impossible to gather data either: (1) on the total number of attacks underway, since not all attacks can be identified at the time of engagement (e.g., zero-day vulnerabilities); or (2) on the number of attacks a fully-protected machine would withstand. The former is impossible both because of the lack of a global structure for comprehensive surveillance and because so-called "zero-

Those attempting to evaluate security effectiveness are faced with the difficult challenge of "proving a negative"—showing that the reason no catastrophic events occurred was the result of onerous security measures. These measurement difficulties, in turn, make quantitatively evaluating the efficacy of regulatory measures based on successes difficult.

This work utilizes an alternate approach, measuring security failures. Rather than looking at reductions in contaminants released or bacterial infestations, it examines security breach incidence. This approach, perhaps akin to measuring incidence of bacterial infestation in infected foodstuffs, attempts to illuminate regulatory efficacy by investigating the degree to which organizations take steps to improve their security measures *after* the introduction of regulation as measured by *reductions* in reported incidents.

A. Tracking Breaches of Personal Information (2000–2010)

Historically there has always been some nominal reporting of security breach incidents. For the purposes of this analysis, a "security breach" constitutes an event involving unauthorized access to sensitive information, primarily as defined by the applicable state SBNs but broadly construed so as to include other incidents that may involve sensitive data but that fail to meet the strict triggering

---

day" attacks, by definition, cannot be detected at the time they are underway (because of the vulnerability they exploit and, therefore, the signature of the attack is known only to the attacker). Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL'Y 63, 64 n.7 (2010) ("A zero-day attack is a previously unseen attack on a previously unknown vulnerability. The term refers to the fact that the vulnerability has been known to the defender for zero days. The adversary has usually known of the attack for a much longer time."). The latter is impossible because a "fully-protected" machine only exists in a vacuum—one completely disconnected from any network and locked in an impenetrable facility. The widely-varying business requirements of operational production environments in organizations require that *some* risk exposure occur; otherwise, it would be impossible for information systems to provide any services. Thus a "control group" against which to test live, production systems cannot effectively be constructed on a global scale. Note, however, that with sufficient public funding, it may be possible to construct an environment that mimics production environments sufficiently to capture data and use for later analysis. While not a control group for the purposes of comparison, such an environment would provide substantial useful information for the purposes of analysis. Currently, however, no such (unclassified) proposals have received sufficient funding to expect this as a usable data source in the near future.

guidelines to contain consumer information. The primary data source is a database of such incidents maintained by the Open Security Foundation.[250] The period of analysis presented here is from January 1, 2000 through December 31, 2010.[251]

Traditional definitions of public versus private sector entities—definitions that rely upon the for-profit status of an organization—do not accurately reflect the demarcations recognized by the various data security laws. Furthermore, following such a strict rule would make examination of the healthcare sector difficult, as organizational boundaries with respect to data ownership are not as clear as organizational boundaries with respect to for-profit status.[252]

Accordingly, the final scope of inquiry extends beyond traditional private firms to include organizations like hospitals and universities. This treatment mirrors that of some state security breach notification statutes, which apply separate requirements to governmental and non-governmental entities, but do not distinguish between for-profit and non-profit organizations.[253] Those states that do not have separate statutes for government organizations also make no distinction between for-profit and non-profit organizations.[254] Post-

250. Open Security Foundation DATALOSSDB, www.datalossdb.org (last visited Jan. 2, 2014). A collection of the incidents reported by the Open Security Foundation is on file with the author.

251. As of late calendar year 2011, the data used in this analysis is no longer being made publicly available by the Open Security Foundation. Repeated inquiries to the curators of the data regarding accessing it for research purposes have gone unanswered. Currently, this dataset is the only (unclassified) one of its kind available in the world.

252. Consider, for example, a research hospital. The hospital itself and any affiliated medical college will be non-profit entities. The physicians within the hospital, however, are likely classified as independent contractors. When practicing medicine at their "private offices," they operate as Professional Corporations, (Limited Liability) Partnerships, and other for-profit organizations under state law. While these two "organizations" are distinct for fiscal purposes, they almost always share patient records. Furthermore, the Health Information Technology for Economic and Clinical Health Act (HITECH Act) effectively requires such information sharing in order to meet certain guidelines for federal funding. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified in scattered sections of 42 U.S.C.).

253. *See, e.g.*, 815 ILL. COMP. STAT. 530/12 (2012) (creating separate statutory notification requirements for state agencies experiencing data breaches and requiring additional reporting, including in some cases to consumer reporting agencies); MASS. GEN. LAWS ch. 93H, § 3(c) (2007) (mandating additional centralized reporting requirements for entities experiencing a security breach if they are state executive branch agencies).

254. *See, e.g.*, HAW. REV. STAT. § 487N-1 (2008) (defining "business" as "a sole proprietorship, partnership, corporation, association, or other group, however organized, and *whether or not organized*

secondary educational institutions, therefore, unlike government institutions, are mostly subject to the same requirements under state breach notification laws as are private firms.[255] Primary and secondary educational institutions, however, are traditionally so interwoven with state and local governments that considering them separately would be difficult.[256] Also included are "general" non-profit organizations such as charitable foundations and research institutions. As with private universities and hospitals, non-profits are treated the same under state security breach notification statutes as are private for-profit entities.[257]

1. Dataset and Variables

The primary dataset comprises a collection of publicly-known security breach incidents maintained by the Open Security Foundation (OSF) known as the DataLossDB database.[258] As described by the OSF:

> DataLossDB is a research project aimed at documenting known and reported data loss incidents world-wide. The effort is now a community one, and with the move to Open Security Foundation's DataLossDB.org, asks for contributions of new incidents and new data for existing incidents.[259]

Until early 2011, the database was an open-source effort, similar to Wikipedia, that relied upon the contributions of individuals worldwide to submit known incidents for review.[260] Only limited

to operate at a profit.") (emphasis added).

255. In some states (e.g., Illinois) state land-grant universities likely fall under the scope of governmental entities. In others (e.g., Massachusetts) they probably do not.

256. Judith A. Winston, *Achieving Excellence and Equal Opportunity in Education: No Conflict of Laws*, 53 ADMIN. L. REV. 997, 1003 (2001) (recognizing that state and local governments are jointly responsible for primary and secondary education).

257. *See, e.g.*, HAW. REV. STAT. § 487N-1.

258. *About OSF Data Loss*, DATALOSSDB, http://datalossdb.org (last visited Jan. 22, 2014).

259. *Id*.

260. *About DataLossDB*, DATALOSSDB, http://datalossdb.org/about (last visited Sept. 17, 2013).

information regarding the methods of collecting data is available, and suggests that the curators rely primarily on news media and public information requests.[261] Although somewhat detailed, these descriptions lack specificity as to the statistical significance of their sampling methods.

This lack of specification as to how incidents are captured does present a methodological problem. As of the time of analysis, however, no better resources were available, and this dataset serves the purpose of allowing analysis on a dataset that at least is likely to exhibit normally distributed error,[262] to the extent error in reporting exists. Notable limitations include the incentive for organizations not to disclose incidents that represent breaches of security but escape the technical reporting requirements (e.g., does not involve a covered combination of personal information but otherwise involve sensitive information) and the fact that there is no baseline for comparison (i.e., there is no database indicating what incidents have *not* been reported). Considering these limitations, as discussed below, the focus on measuring only relative changes over time is appropriate.

2. Analysis Groups: Previously Regulated and Previously Unregulated Entities

Categorizing existing information security law and regulation into two groups allows the empirical comparison of the efficacy of those styles of regulation. The first group, directive regulation, comprises the state Security Breach Notification laws (SBNs), and the second group, Management-Based Regulatory Delegation, comprises HIPAA, GLBA, and the FTC's Section 5 privacy and information security enforcement activity. The chronological order in which these statutes were enacted allows quantitative comparison of their efficacy

261. *See id.*

262. Each of the SBNs are laws of general applicability and, thus there is no reason to believe any industry will have a reporting bias as a function of lack of access to reported incidents. For the purpose of this analysis, I assume that all actors are rational with respect to reporting incidents as required under the law *once the organizations become aware of their reporting obligations*, a condition not necessarily coincident with when those organizations actually became subject to those obligations.

by grouping organizations into two classes based on the type(s) of regulation to which they were subject at various points. HIPAA was enacted in 1996,[263] and the Final Security Rule took effect in 2003.[264] GLBA was enacted in 1999,[265] the Interagency Guidelines became effective in 2001,[266] and the Safeguards Rule became effective in 2003.[267] The state SBNs varied in their effective dates, beginning in 2003 with many being enacted toward the end of the decade.[268] The FTC's privacy and data security enforcement, as discussed in Part II,[269] began in 2000 but did not substantially gain traction or attention among regulated entities until much later in the decade, as discussed in Part IV.[270]

SBNs are the primary drivers of security incident reporting in the United States and were introduced in large scale several years after the effective dates of HIPAA and GLBA.[271] This chronology suggests grouping organizations according to whether they were previously subject to regulation at the time SBNs began to drive reporting. The first group, Previously Regulated Entities (PREs), comprises organizations primarily in the healthcare or finance sectors that were subject to HIPAA or GLBA prior to the introduction of SBNs. The second group, Previously Unregulated Entities (PUEs), comprises organizations in most other sectors which previously were not subject to information security regulation.[272] Because the FTC's

263. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.).

264. 16 C.F.R. § 314.5(a) (2013).

265. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., 16 U.S.C., 18 U.S.C., and 29 U.S.C.).

266. 12 C.F.R. § 30, App. B § (III)(G) (2013).

267. 16 C.F.R. § 314.5(a) (2013).

268. *State Security Breach Notification Laws*, *supra* note 41.

269. *See* discussion *supra* Part II.

270. *See* discussion *infra* Part IV.

271. *State Security Breach Notification Laws*, *supra* note 41.

272. While some limited corner cases existed, including Department of Defense regulations, IRS regulations, and those few organizations that drew the attention of the FTC in the early 2000s, these instances are so small as not to bias the analysis. Furthermore, at that point in time—particularly with large organizations at a time when security was not taken seriously as a business need—it would be difficult to assume that such limited-scope regulations would be likely to drive costly, organization-wide

enforcement jurisprudence did not appear to gain attention among regulated entities until late in the 2000s, it is excluded as a category for the purpose of quantitative analysis.[273]

As of February 17, 2011, the DataLossDB dataset contained 3,076 breach reports from January 1, 2000 through December 31, 2010.[274] 2,575 were experienced by organizations in the United States.[275] Of these, 2,107 fit the criteria described above.[276] 810[277] were from previously-regulated industries and the remaining 1297 were from previously-unregulated industries.[278]

3. (Three) Trends in Breach Incidence

Analysis of breach incidence from January 1, 2000 (t_0) through December 31, 2010 (t_F) revealed three trends in periodic breach incidence. The first trend is an initially low (and not statistically significant) rate of reporting. This trend continues until approximately Summer 2004 (t_1), and describes a period prior to the introduction of SBNs when organizations lacked incentives to report and therefore only minimal reporting (or other discovery) of security events occurred.

The second trend comprises a substantial rise in reporting rates, lasting until approximately Summer 2008 (t_2), and describes a period during which SBNs started to become effective in various states and organizations began reporting. During this period, reporting is assumed to be incomplete either because organizations experiencing incidents were not yet subject to SBNs or because they were unaware of the reporting requirements of SBNs. No useful data is currently available on the knowing disregard of reporting requirements, so this

practices. The interviews with CISOs, discussed in detail in Part IV, support this hypothesis.

273. If the Open Security Foundation data becomes available again, or another data source is developed, analysis of more recent years' activity may be informative as to the effects of FTC enforcement as it gained awareness among organizations subject to the Commission's jurisdiction.

274. *See supra* note 250.

275. *Id.*

276. *Id.*

277. 354 are from financial sector organizations, and 456 are from healthcare sector organizations. *Id.*

278. *Id.*

variable is assumed to be uniformly distributed and excluded from analysis. The mere presence of substantial regulation (and the legislative history behind the regulation, as discussed in Part II) suggests discounting the possibility that no incidents occurred prior to t_1 as an explanation for this trend.

The third trend comprises the period from t_2 through the end of the analysis period (t_F), and describes a period during which the incidence of reported breaches *decreased*. This period begins at the point (t_2) at which organizations are believed to be aware of their reporting obligations under SBNs and all organizations required to report are doing so.

Unlike most laws passed on a state-by-state basis, the triggering of a notification statute is based neither on the residence of the organization experiencing the breach nor on the location where the event took place. Rather, the triggering of a notification statute is based on the residence of individuals described in the lost data.[279] This information is a function of the composition of the dataset breached, and while the size (number of individuals whose information was compromised) is released under many SBNs, the composition of those individuals (i.e., their state of residence) is not.[280] Thus, information about which states' laws would be triggered is completely endogenous to each incident listed in the database.[281] Therefore unlike with traditional state-by-state analysis where one looks to the domicile of a firm to determine if it is affected by

279. *See, e.g.*, N.J. STAT. ANN. § 56:8-163(a) (West 2006) (requiring notification "to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person"); 73 PA. CONS. STAT. § 2303(a) (2006) (requiring notification to any resident of Pennsylvania).

280. Nor can the residence be inferred, because information about the residence of the individuals is neither broken out comprehensively by state under any individual state statute's central reporting requirement nor do all states have centralized reporting requirements. Currently only 14 of 46 states with SBNs require centralized reporting (notably, New York's statute *does* mandate centralized reporting). *See State Security Breach Notification Laws*, *supra* note 41.

281. More specifically, such information is endogenous to the incident itself (as opposed to the record in the database) and is reported neither in the record in the database nor in the primary sources often cited in each record. While there are a (sparse) few incidents for which such information is reported, these represent only a fraction of overall incidents and are therefore not useful for addressing this problem.

regulation it is impossible for the outside observer to make such a determination.

The inflection points t_1 and t_2, which demarcate the trends in breach incidence, are derived from polynomial regression analysis. Polynomial regression analysis allows a curve (as opposed to a straight line) of "best fit" to be determined for a set of data over an extended period of time. Comprehensive analysis of polynomials of orders 2 through 10 revealed that order 5 polynomials provided the statistically best fit for describing trends in breach incidence for organizations in both the PRE and PUE groups.[282] The following figures depict the results of those regressions:

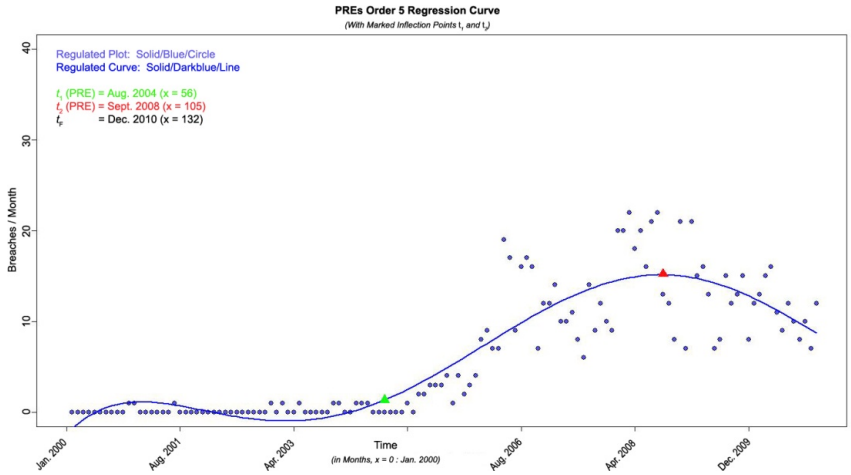


Figure 1—Polynomial Regression Curve of Order 5 for PRE Breach Incidence

282. A complete and comprehensive description of this analysis, the procedures used, and the results are discussed in another work. *See* Thaw, *supra* note 55, at apps. A–A.6.

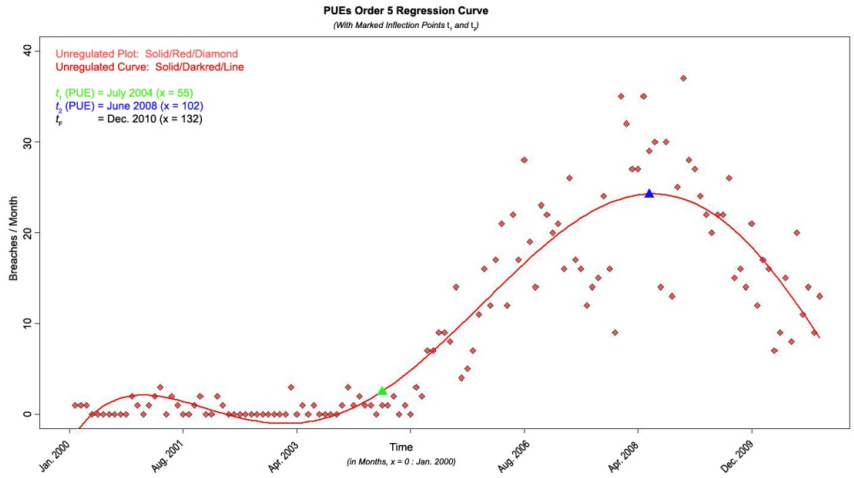


Figure 2—Polynomial Regression Curve of Order 5 for PUE Breach Incidence

While the points t_1 and t_2 vary slightly for PREs and PUEs, this variance is within an acceptable margin of error both for the regressions used and considering periodicity. This discrepancy therefore does not suggest treating the two categories separately for the purposes of analyzing the impact of regulation on security outcomes.

B. Blended Regulation is Optimal at Preventing Breaches

Based on the trend periods established through the above methods, I conducted analysis comparing PREs and PUEs during these periods. The results suggest that a blend combining both directive regulation and Management-Based Regulatory Delegation is optimal for incentivizing organizations to employ security measures to prevent security breaches involving sensitive personal information.

This analysis examines the period after SBN compliance reached saturation (t_2). At this point, all firms reporting incidents are assumed to be aware they are subject to SBNs and reporting all applicable incidents in good faith. Firms are assumed to have strong incentives to reduce the number of reportable incidents they face. In addition to the negative public relations potential, some studies have reported

negative effects on stock price and firm performance following incident reports (although the data is admittedly mixed)[283] and the interviews discussed in Part IV further suggest organizational incentives to avoid reporting.[284]

Thus, if t_2 represents the point at which no further increase in reporting will occur due to other organizations learning of their reporting obligations, it follows that from t_2 through t_F (and beyond) there should be a decreasing trend in breach incidence. This trend will primarily result from organizations taking security measures to reduce the number of reportable incidents they experience. Comparing the trends during this period between PREs and PUEs provides insight into the efficacy of directive regulation and Management-Based Regulatory Delegation at preventing breaches of personal information.

With an established compliance saturation date for SBN reporting (t_2), linear regression from this point can provide more detailed insight comparing these trends. The following figure and table depict the results of these regressions and their statistical significance:[285]

283. *See generally* Alessandro Acquisti, Allan Friedman & Rahul Telang, Is There a Cost to Privacy Breaches? An Event Study (2006) (unpublished manuscript prepared for Twenty Seventh International Conference on Information Systems), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf; Myung Ko & Carlos Dorantes, *The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation*, 17 J. INFO. TECH. MGMT. 2 (2006), *available at* http://jitm.ubalt.edu/XVII-2/article2.pdf.

284. *See* discussion *infra* Part IV.

285. A complete and comprehensive description of this analysis, the procedures used, and the results are discussed in other work. Thaw, *supra* note 55, at 89–94.

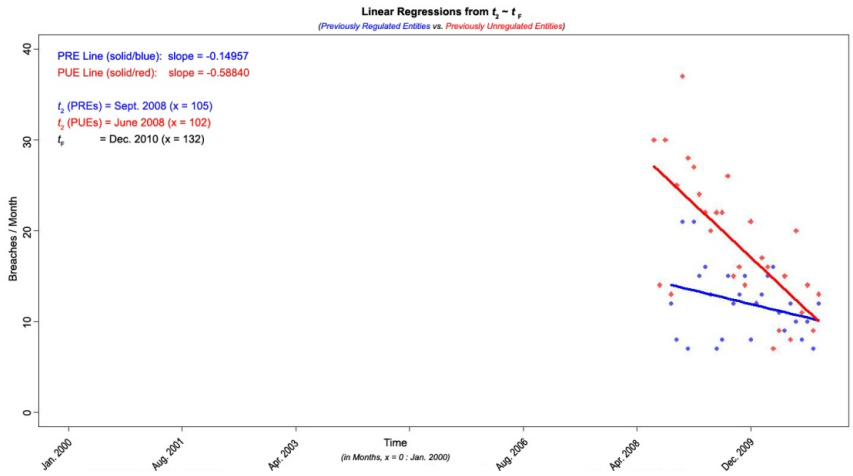


Figure 3—Linear Regressions of PRE and PUE Breach Incidence from t_2 *to* t_F

Statistical Data	PRE Linear Regression (t_2 to t_F)	PUE Linear Regression (t_2 to t_F)
Residual Std. Error	3.759 (on 25 DF)	5.507 (on 28 DF)
Adj. R-Squared	0.05776	0.4596
p-value	0.1198	$2.318 * 10^{-5}$
Intercept [sig.]	29.87322 [*]	87.7074 [***]
Coefficient x [sig.]	-0.14957 [ ]	-0.5884 [***]
Significance Codes: *** (0.001) ** (0.01) * (0.05) . (0.1) [blank] (1)		

Table—Summary of Key Statistical Information from Linear Regressions[286]

The two sections that follow explain the implications of these trends for the regulatory efficacy and suggest why a blended regulation model is optimal at preventing breaches of personal information.

286. The weaker statistical significance reported for the PRE regression line is due to periodicity selection effects. Observation of the (calendar) monthly incidence of breaches for PREs around the time of t_2 indicates several outlier months. Additionally, testing not yet reported as of the time of this writing indicated stronger statistical significance with refined approaches to the period for grouping incidence.

1. Blended Regulation Compared to Directive Regulation Alone

The effects of blended regulation, or a combination of directive regulation and Management-Based Regulatory Delegation, are measured by the decreasing trend in breach incidence after t_2 for PREs. After t_2, PREs—generally healthcare and finance organizations—were subject not only to their respective forms of Management-Based Regulatory Delegation (HIPAA or GLBA), but also to the state SBNs.[287] Like all organizations, they have an incentive to reduce their reportable incidents by implementing security measures to prevent reportable breaches. Thus, the downward trend (represented by the blue linear regression line in Figure 3) represents how rapidly PREs reduced their reportable incidents.

The rate at which PREs reduced their reportable incidents was nearly four times less[288] than the rate at which PUEs (represented by the red linear regression line in Figure 3) decreased their reportable incidents. At first glance, this might appear as though Management-Based Regulatory Delegation was detrimental, as PREs reduced incidents at a slower rate than did PUEs. Paradoxically, however, the opposite is true.

There is no evidence that organizations' incentives to reduce security breach incidents vary by industrial sector. If there were such variance, however, it would likely indicate that the finance and healthcare sectors had higher incentives than the collective remainder of industry as those sectors traditionally handle more sensitive information. Additionally, there is no control data against which to compare breach incidence—thus there is no method to determine whether certain sectors were subject to more attacks than were other sectors. The compliance saturation point (t_2), however, provides a method by which to infer comparative competency.

---

287. *See State Security Breach Notification Laws*, *supra* note 41, for a current list of state SBNs.

288. As listed in Table 1, the slope of the PRE regression line was -0.14957 and the slope of the PUE regression line was -0.5884, representing a 3.9339 times greater rate of decrease.

If incentives and available resources to reduce breaches are equal, and there is a limited total reduction in breaches that can be achieved (perfect security is, as discussed above, impossible), then the rate of decrease after t_2 will be inversely proportional to organizations' *prior* effectiveness at preventing breaches. In other words, organizations already possessing information security competencies will experience a *less rapid* drop-off in breach incidence reporting after t_2 *because they had less far to improve* (i.e., they were already some percentage of the way there). By contrast, organizations that had none or minimal information security measures in place prior to the influence of SBNs (at time t_2) will experience a more rapid decrease (i.e., because they had "further to go").

Thus the results reported here suggest that the combination of directive regulation and Management-Based Regulatory Delegation, at least over the short term, may be as much as four times more effective at preventing breaches of personal information as is directive regulation alone. Over the longer term, the trends may suggest that both organizations will develop sufficient competencies (assuming the regulatory penalties are sufficient), however this finding has strong implications for any new subject of regulation seeking shorter-term efficacy.

2. Blended Regulation Compared to Management-Based Regulation Alone

The effects of blended regulation, or a combination of directive regulation and Management-Based Regulatory Delegation, are measured by the decreasing trend in breach incidence after t_2 for PREs. The decreasing trend in breach incidence suggests that organizations made efforts to improve their information security practices and reduce reportable security breach incidents. The fact that after t_2 PREs still exhibited a decreasing rate of breach reporting suggests they still had "room to improve," notwithstanding their prior experience being regulated by HIPAA and/or GLBA.

While the exact degree of improvement is more difficult to quantify than the first comparison, due to the lack of a control group,

the decreasing trend clearly indicates the addition of directive regulation—specifically the SBNs—improved healthcare and finance organizations' information security capabilities at preventing breaches of sensitive personal information.

C. Analytical Limitations and Future Research

Before proceeding to suggest conclusions from this quantitative analysis, certain shortcomings should be noted. First, the analysis depends on comparing rates of change in reducing breach incidence. For the reasons discussed above, measuring relative rates of change is superior to measuring absolute values. However, the use of relative rates of change assumes a degree of consistency in organizational incentives to reduce breach reporting. While a facially reasonable assumption, when sufficient data is available to measure organizational incentives in this regard, the relative-rates-of-change analysis should be revisited.[289]

Second, the linear regressions that form the basis for the rates-of-change analysis depend on the selection of proper inflection points. As noted above, and as discussed further elsewhere,[290] the polynomial regression approach employed to determine the inflection points likely provides reasonable estimates both of when organizations began to report incidents (t_1) and of when organizations reporting reached "full compliance" (t_2). However, randomized variation of these two values during the analysis process demonstrated that moderate variance can alter the comparative difference between the rates-of-change post-full-compliance. In all cases the PREs had a statistically significantly shallower slope (i.e., they still had "less far to go" and thus were likely "better prepared");

289. Pending ongoing availability of breach incidence data—which may be available from a new source now that the Open Security Foundation has stopped releasing its dataset (the Privacy Rights Clearinghouse is reviving its aggregation of this data, see https://www.privacyrights.org/data-breach)—the author anticipates proceeding with further analysis on rates-of-change with updated data. Even without other data on organizational incentives, additional time-series data on breach incidence is likely to provide further insight into the validity of the rates-of-change analysis approach.

290. *See* Thaw, *supra* note 55, at apps. A–A.6.

however, over a longer time frame this trend bears further investigation.

Finally, this dataset—as with many datasets—may be subject to reporting bias. There is no evidence to suggest it is biased—rather the contrary—many incidents made it into the dataset *before* they were publicly reported pursuant to state Security Breach Notification laws.[291] Nonetheless, the limitations of an informally-compiled dataset should be noted. As discussed elsewhere, to-date no better unclassified dataset exists for this analysis, and the author suggests that lawmakers and regulators may wish to encourage the collection of such information.[292]

While these limitations do suggest the need for further research when better data becomes available, they do not limit the results of this analysis such that the conclusions are invalid. A finding, for example, of only twice the rate-of-change between PREs and PUEs would still suggest a substantial (and statistically significant) difference between the efficacy of the respective regulatory regimes. Thus the purpose of this section is to identify limitations and suggest future research to improve this work, not that the ultimate policy recommendations are necessarily weakened if the limitations here were ultimately found substantial.

D. Conclusions from Quantitative Analysis

The quantitative analysis presented here suggests two conclusions. First, legislators and regulators should consider the addition of performance-based standards, through directive regulation, to

291. The author is personally aware of such incidents, but cannot disclose further details without violating human subjects research protocols and/or attorney-client privilege. *See infra* note 300.

292. *See Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce*, 113th Cong. (July 18, 2013) (Testimony of David Thaw, Visiting Assistant Professor of Law, University of Connecticut)). For an executive summary, see ENERGY & COMMERCE COMM., *Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?: Executive Summary of Written Testimony of Dr. David B. Thaw* (July 18, 2013), *available at* http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Thaw-CMT-Data-Breaches-Consumer-Protection-2013-7-18.pdf.

existing regulatory regimes relying on forms of management-based regulation. In the United States, we have seen such activity in recent years, with the Department of Health and Human Services adding a breach notification requirement to HIPAA[293] and the Securities and Exchange Commission issuing guidance suggesting that publicly-traded companies disclose material security incidents in their quarterly filings.[294] Outside the United States, regulators in areas such as Europe—which employ complex privacy and information security regulatory regimes, but as of yet do not have comprehensive breach notification requirements[295]—may wish to consider introducing such requirements.

Second, the additional competency Previously Regulated Entities demonstrated suggests that regulators may wish to expand the reach of Management-Based Regulatory Delegation models to other industrial sectors. The FTC's Section 5 privacy and information security enforcement jurisprudence may produce such an effect; however, it is primarily reactive. Some legislative proposals have been put forth to give the FTC prospective rulemaking authority in this regard,[296] though none have yet gained traction.

Outside the information security space, regulators may wish to consider blended regulation as an approach for two reasons. First, organizations previously subject to Management-Based Regulatory Delegation exhibit greater competency to adapt to new performance-based or other prescriptive regulation when they are subsequently adopted.[297] Second, the addition of performance standards may be used to achieve marginal improvements in key regulatory areas where a delegation model fails to achieve desired outcomes—such additions effectively grant regulators the flexibility to "nudge"

293. Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, § 13402, 123 Stat. 115, 260-63 (2009) (codified as amended in 42 U.S.C. § 17932 (2012)).

294. *CF Disclosure Guidance: Topic No. 2, Cybersecurity*, U.S. SEC. & EXCH. COMM'N (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

295. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 159, at 276.

296. *See, e.g.*, Data Accountability and Trust Act (DATA) of 2011, H.R. 1841, 112th Cong. §§ 2(a)(1), 3(d)(3), 3(f)(2)(B), 4 (2011).

297. *See supra* note 258 and accompanying text.

regulated entities toward goals without removing entities' discretion in heterogeneous industries. It is important to note, however, as discussed further in Part IV, that certain forms of directive regulation which specify means of performance (or means to avoid penalties) may actually reduce the discretion desired of management-based regulatory approaches.[298] Regulators must consider this balance when adopting new forms of directive regulation to supplement existing Management-Based Regulatory Delegation.

IV. QUALITATIVE ACCOUNTS OF REGULATION AS DRIVING SECURITY

A. Views from Chief Information Security Officers

In a field lacking substantial empirical data or other literature upon which to draw, qualitative methods may often form an effective tool to inform initial research directions. Chief Information Security Officers (CISOs) are the key individuals within large organizations responsible for directing the security policies and practices of the organization and advising senior management on decisions affecting security risk management. They are on the leading edge of implementing information security regulatory compliance objectives.

The qualitative data comprises a series of two-hour semi-structured interviews with Chief Information Security Officers.[299] These interviews were designed to provide insight and intuition about how regulatory models affect security practices and how those models bring about change. Given the absence of prior literature upon which to draw to formulate research questions, the results of these interviews served both as a direct data source and as a means to help develop the theoretical framework in Part II and the quantitative methods used in Part III.

298. *See infra* Part IV.

299. A complete and comprehensive description of this analysis, the procedures used, and the results are discussed in other work. Thaw, *supra* note 55, at 94–107.

The requirements for protection of human subjects in research under federal guidelines[300] require that an Institutional Review Board (IRB) review and approve of a protocol for the protection of human subjects prior to their participation in research. The overseeing IRB for the CISO interviews was the University of California, Berkeley's Committee for the Protection of Human Subjects (CPHS). The protocol approved by CPHS for this research project requires full anonymity of the subjects interviewed, as their responses have the potential to affect their employment adversely.[301] Accordingly, while the author and his co-researchers maintain copies on-file of the transcripts, the author cannot disclose those transcripts, the identities of the subjects (beyond the general descriptions provided herein), or provide copies of the transcripts to the *Georgia State University Law Review*.

Interview subjects were recruited from large organizations in the healthcare, finance, information systems and technologies, consumer products, and public utilities sectors. Interviewees needed to be the CISO of their organization or business unit, or the functional equivalent thereof. Selected subjects included CISOs of:

1. a major computer hardware manufacturer;
2. a major financial services provider;
3. a major software and internet applications provider;
4. a major telecommunications provider;
5. a major research university (with a substantial medical research campus);
6. a major healthcare services provider;
7. a major health insurance carrier;
8. a major pharmaceutical firm; and

300. National Research Act of 1974, Pub. L. No. 93-348, 88 Stat 342 (1974); Protection of Human Subjects, 45 C.F.R. pt. 46 (2009); *Office for Human Research Protections (OHRP)*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ohrp (last visited Jan. 5, 2014).

301. Comm. for Prot. of Human Subjects, CPHS Application 5–7 (2007) (unpublished research project application materials, University of California, Berkeley) (on file with Georgia State University Law Review).

9. a major provider of healthcare information technology.

The interviews were conducted over a two-year period through 2008 and 2009. In addition to contributing to the theoretical framework and quantitative analysis, the results of the interviews yielded two direct findings. First, that directive regulation like SBNs decrease the importance of technical professionals[302] within the organization, whereas Management-Based Regulatory Delegation like HIPAA, GLBA, and the FTC's enforcement actions increase organizations' reliance on technical professionals because such organizations' general management appear to lack the technical expertise to make judgments as to "reasonableness" on technical matters.[303] Second, that a lack of guidance from regulators defining "reasonableness" within the context of information security leaves CISOs unable to justify requests for additional resources or imposition of onerous security practices necessary to meet compliance obligations.[304]

B. Effects of Regulation on Organizational Roles: Locking The Bank or Vault Door and Leaving the Back Window Open

The most desirable types of relationships between managers and professionals within organizations depend on the structure of the organization. Most of the organizations represented by the CISOs interviewed for this work employ structures based upon Fordist/Weberian "command-style" management hierarchies.[305]

302. Within this context, the term "professional" refers to what law traditionally considers "learned professionals," such as physicians, attorneys, accountants, engineers, and scientists. It specifically does not refer to vocationally trained technicians. Within the information security context, learned professionals generally would include senior management-level executives with a strong technical background and expertise tasked with planning and high-level advising, as opposed to vocationally-trained technicians responsible for operating and configuring security technologies in response to high-level directives. This distinction, while easily articulated, is admittedly difficult to draw in practice, in large part due to the lack both of formalized education in cybersecurity and of formalized *licensure* (as opposed to vocational certification) as discussed in Part II above.

303. Thaw, *supra* note 55, at 118.

304. *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 159, at 291.

305. *See generally* W. RICHARD SCOTT & GERALD F. DAVIS, ORGANIZATIONS AND

There are four conditions necessary for such organizations to function effectively. First, supervisors must be able to know when their subordinates are wrong about something.[306] Second, supervisors must know how to correct subordinates' mistakes.[307] Third, subordinates must be fungible—there must be a market for other professionals of equal or greater ability to replace them.[308] Fourth, and finally, the consequences of subordinates' errors must be readily apparent and those consequences able to be connected to particular actions on the part of the subordinate.[309] Modern organizations, however, have evolved to understand the need for senior managers to rely upon the judgment and discretion of technical professionals.[310]

1. Directive Regulation: SBNs Decrease Reliance on Technical Professionals

Current SBNs—the predominant form of directive regulation in information security—exempt from the regulatory penalty of disclosure any security breach where the data compromised was encrypted.[311] The result, as discussed earlier, is *de facto* means-based regulation under which regulated entities respond to the performance standard by adopting practices to ensure the penalty exception. As explained by one CISO of a large healthcare organization:

ORGANIZING 46–50 (2007).

306. These criteria were developed with Professor Todd LaPorte (University of California, Berkeley, Department of Political Science) and are partially derivative from the following works: SCOTT & DAVIS, *supra* note 305, at 124–82; JAMES D. THOMPSON, ORGANIZATIONS IN ACTION 117–41 (2007).

307. SCOTT & DAVIS, *supra* note 305, at 124–82; THOMPSON, *supra* note 306, at 117-41.

308. SCOTT & DAVIS, *supra* note 305, at 124–82; THOMPSON, *supra* note 306, at 117-41.

309. SCOTT & DAVIS, *supra* note 305, at 124–82; THOMPSON, *supra* note 306, at 117-41.

310. SCOTT & DAVIS, *supra* note 305, at 148 ("[A]s levels of complexity, uncertainty, and interdependence increase, 'independent' professionals are likely to move their work into organizational structures, thus becoming components of a wider division of labor and increasingly subject to more formalized coordination mechanisms.").

311. *See, e.g.*, CONN. GEN. STAT. § 36a-701b(a) (2006) (defining "breach of security" as "unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data containing personal information *when access to the personal information has not been secured by encryption* or by any other method or technology that renders the personal information unreadable or unusable") (emphasis added).

> . . . [SBNs] caused us to . . . in a very short period of time, encrypt 40,000 laptops [with] whole disk encryption . . . .[312]

The CISO of a large telecommunications company also described the move toward encryption:

> [W]hat we have done is all computers now have to be encrypted.[313]

In total, 5 of the 9 respondents[314] also identified SBNs as playing a substantial role in driving their information security practices. One respondent, from a financial services organization, remarked about the straightforward character of SBNs regulatory requirement:

> . . . [D]espite my reservations about [California's breach notification law], on which most of the breach notification legislation has been modeled, it was exemplary in one regard . . . it was an extremely small piece of legislation.[315]

Ironically, while this CISO found the simplicity appealing, it was this simplicity that decreased the need for managers to rely on technical professionals' discretion and judgment. As stated by one CISO of a large healthcare organization:

> And so what's been really interesting about the Notification Laws is [they] have come in and [ ] essentially reversed the whole direction security was taking from when I started this job.

312. Thaw, *supra* note 55, at 97.
313. *Id.*
314. In the context of qualitative semi-structured interviews, this finding is significant. The interview structure did not specifically ask about SBNs, but rather—through a natural discussion style—encouraged interviewees to discuss the subjects most relevant to them. Interviewees were, in fact, directly told that the researchers are here for them to tell what is most relevant to the interviewee. In this format, interviewees are likely to focus extensively on certain topics, and the fact that over half the interviewees focused on SBNs is a very significant finding.
315. Thaw, *supra* note 55, at 104.

> [The original direction was] we're going to figure out the privacy side of it . . . but we're also going to build up capabilities to stop the cyber apocalypse because we're worried about that sort of thing after September 11th and also because network security attacks are getting increasingly sophisticated. We have to build up the tools and the talents in our shops where we don't have any of them and we can't afford to pay [for] them. We have to do it ourselves.[316]

This respondent describes a shift from an original direction where the security team "ha[d] to do it [them]selves" to a new, "reversed" direction.[317] The respondent goes on to say:

> So what's happened since the Notification Laws have become sort of ubiquitous in the last three years [is] the security investment is moved, essentially to crypto. If it moves, encrypt it. It if stays there, encrypt it. There's not much reflection on whether or not actually anyone ever uses that data.[318]

Here, the respondent describes the effect of directive regulation with performance standards tied to specific means (the SBNs) in decreasing their organization's reliance on the professional's exercise of discretion. This condition is well-suited to command-style hierarchies because clear, absolute standards (like the encryption exception in SBNs[319]) create measured outcomes by which managers can identify and correct the mistakes of subordinates.[320]

---

316. *Id.*at 121–22.
317. *Id.*
318. *Id.*
319. But note the lack of definition as to what constitutes "encryption." Under the existing statutory language, a lost laptop containing two versions of a file with personal information, each of which was encrypted using Microsoft Office 2003's implementation of RC-4, would likely satisfy the statutory definitions referenced *supra* note 138. This particular implementation of RC-4, while operating at a 128-bit encryption key length, has a known vulnerability under which an attacker can break the encryption with minimal effort. Hongjun Wu, *The Misuse of RC4 in Microsoft Word and Excel*, CRYPTOLOGY EPRINT ARCHIVE (Jan. 10, 2005), *available at* http://eprint.iacr.org/2005/007.
320. *See supra* notes 306–09.

The result, as apparent from the quotes above, is a condition in which organizations (presumably at the direction of senior management) focus substantial energy on avoiding the regulatory penalty by adopting the means-based exception. It is important to note, however, that this condition may not be inconsistent with the original intent of the statutes—to protect sensitive consumer data and reduce incidence of identity theft.[321] If data is properly encrypted, even if lost, it poses no plausible threat to consumers.

This result, however, only focuses on one potential threat—unencrypted data. If left to their professional discretion, CISOs might well (and probably would) choose to focus on multiple threats.

2. Management-Based Regulatory Delegation: HIPAA and GLBA Increase Reliance on Technical Professionals

While perhaps better-suited to the most common types of organizational structures in place in the United States, directive regulation may pose other risks for the organization by reducing its capacity to leverage the flexibility afforded by Management-Based Regulatory Delegation. Though the addition of performance-based standards specifying specific means does not reduce the compliance obligations of management-based models, it may reduce the available resources to implement the compliance plans developed under those models. This resource limitation may contribute to a regulatory "race to the bottom."

Consider the advantages respondents identified afforded by the flexibility of a Management-Based Regulatory Delegation model, as described by the CISO of a large healthcare organization:

> They [the Department of Health and Human Services] stayed technology-neutral. They didn't specify exact levels of

321. *See, e.g.*, Data Accountability and Trust Act (DATA) of 2011, H.R. 1841, 112th Cong. (2011) ("To protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach.").

> encryption. They didn't specify exact methods of user authentication. A lot of that was in the proposed rule, and they very rightly took it out.[322]

Another CISO similarly reported their experiences consulting with the National Committee on Vital and Health Statistics:

> . . . meeting with some folks at NCVHS . . . because they have a mandate to report back to HHS to determine whether or not there ought to be any changes to the regulations . . . .And [we were discussing whether] to expand the scope of these safeguards to apply to de-identified data to avoid some of these risks that we [respondent's organization] were open to it not only because we think we do those things today, but it might be an important thing to do from their standpoint and from a policy standpoint to ensure that it isn't just the companies like ours that think about these things all the time, but that everybody is put on notice that this is a good practice.[323]

All the CISOs interviewed from the finance and healthcare sectors expressed either a direct or indirect appreciation for their ability to participate in the rulemaking process for information security regulations. They remarked that the flexibility afforded by the regulations, in particular HIPAA, afforded them the ability to meet regulatory goals while still focusing on the security needs most salient to their organizations.

Although highly favored by the respondents, regulation that encourages reliance on professional discretion is disruptive of command-style hierarchical relationships because it necessarily creates an environment in which managers both are unaware of and

322. Thaw, *supra* note 55, at 120.

323. *Id.* at 115. HIPAA required—as part of its regulatory delegation component—that regulators consult with and, subject to limited exception, accept the recommendations of the NCVHS as part of the rulemaking process. *See supra* text accompanying note 110. *See also* David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. (forthcoming 2014).

are unable to correct their subordinates' (technical professionals) mistakes. The risk analysis and implementation details of information security are highly technical. It is nearly impossible for senior managers, charged with overseeing the operations of an entire organization, to maintain the knowledge necessary to correct their subordinates' mistakes.

This risk, however, must be considered against the risk of handicapping technical professionals' ability to identify and address the most salient security risks. The analysis in this section suggests that the style of regulation substantially impacts the role and influence of technical professionals. To paraphrase one CISO, "we need tools and talents to defend against the cyber apocalypse (multiple threats) . . . and we can't afford to pay for them."[324] Thus, if regulation's impact on the role of technical professionals within organizations is ignored, regulators run the risk of ensuring the bank or vault door is well-secured (data is encrypted) and the back window is wide open (every other information security threat remains insufficiently addressed). I do not suggest that this risk is dispositive of increasing the use of directive regulation, only that its implementation should be considered with care to avoid the risks outlined here. Technology-neutral directive regulation, for example, or that which references standards developed (and perhaps more importantly, updated) by organizations like the National Institute for Standards and Technology (NIST), may provide steps toward such flexibility.[325]

C. Unreasonable Deficiencies in "Reasonableness:" Lack of Clarity Impedes Compliance Efforts

When regulation weakens CISOs' ability to exercise their professional judgment as to the greatest threats facing the

324. Thaw, *supra* note 55, at 121–22.

325. *See, e.g.*, NAT'L INST. OF STANDARDS & TECH., ANNOUNCING THE ADVANCED ENCRYPTION STANDARD (AES), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 197 (2001), *available at* http://www.nist.gov/itl/upload/fips-197.pdf.

organization, many salient risks may remain unaddressed. The result may be a "race to the bottom," in which organizations adopt and implement compliance plans at the bare minimum level they believe will pass regulatory muster. This condition may result not as a function of intended regulatory evasion, but rather as a result of a redirection of resources to one specific threat (as described above) and an inability of the CISO to justify requests for additional funding due to a lack of specificity as to what constitutes "reasonable" in the context of regulatory requirements.

Examples of this "race to the bottom" pervade regulatory enforcement actions. Many of the most notable FTC information security enforcement actions comprise security failures so irresponsible and obvious that the affected entities' names have become synonymous with information security deficiency.[326] Such low-hanging fruit continues to be available to regulators today.[327]

Current information security regulation relies heavily on a concept of reasonableness—in developing compliance plans consistent with the Management-Based Regulatory Delegation models, organizations must make judgments regarding what constitutes "reasonable security." This is particularly true for HIPAA compliance, where compliance obligations almost always scale to the size, scope, and complexity of the organization.[328]

When combined, these factors yield a perfect storm for the regulatory "race to the bottom." Directive regulation drives perhaps-otherwise-sufficient security budgets toward specific compliance objectives, such as encryption. This, in turn, reduces the available resources for other security activities and forces CISOs to focus on meeting minimum compliance objectives rather than prioritizing the greatest threats they feel their organizations face. With an abundance

326. *In re* TJX Cos., No. C-4227, 2008 WL 3150421, at *2–3 (F.T.C. July 29, 2008); *In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 WL 2395788, at *1–2 (F.T.C. Sept. 20, 2005). Multiple CISO respondents specifically mentioned T.J. Maxx Cos. (TJX) when discussing security failures and the costs thereof, specifically associating the company with security deficiencies.

327. *See, e.g.*, *In re* Twitter, Inc., No. C-4316, 2011 WL 914034 (F.T.C. Mar. 2, 2011).

328. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1173(d), 110 Stat. 2025–26 (codified as amended at 42 U.S.C. § 1320d-2(d) (2006)).

of low-hanging fruit available to regulators—even if likely through malfeasance, not misfeasance—the bar is set extremely low. Thus, regulators are faced with an industry standard set perhaps below their optimal level. As long as low-hanging fruit remains available to regulators, CISOs will not be able to justify requests for new resources on the grounds that peer organizations with comparable policies have been subject to enforcement action. Nor will they be able to justify requests based on the regulations themselves, as "reasonable" lacks an operational definition any higher than the low-hanging fruit provided by cases such as *B.J.'s Wholesale Club*,[329] *T.J. Maxx Cos.*,[330] and *Twitter*.[331] And so the cycle continues.

This analysis strongly suggests the conclusion that regulators provide more proactive guidance as to what constitutes "reasonable" standards for security practice. This is, perhaps, not as difficult a challenge as some of the CISO respondents might suggest. While including exact encryption specifications in the promulgated regulations is likely inefficient, referencing current standards on encryption, such as those promulgated by NIST, provides an excellent, flexible, and adaptive solution.[332] Developing standards is among NIST's core competencies, and it publishes Federal Information Processing Standards on a wide variety of topics,[333] including encryption.[334] Some legislative proposals have considered giving the FTC proactive rulemaking authority with respect to information security.[335] Such federal legislation may be well-served to instruct the Commission that its rulemaking reference standards clarifying concepts of reasonableness within information security. Regulators in other substantive areas facing a structurally similar lack

329. *BJ's Wholesale Club*, 2005 WL 2395788.
330. *TJX Cos.*, 2008 WL 3150421.
331. *Twitter, Inc.*, 2011 WL 914034.
332. *See* ADVANCED ENCRYPTION STANDARD, *supra* note 325.
333. *Computer Security Resource Center, Publications*, NAT'L INST. OF STANDARDS & TECH., http://csrc.nist.gov/publications/PubsTC.html (last updated Dec. 2, 2013).
334. ADVANCED ENCRYPTION STANDARD, *supra* note 325.
335. Data Accountability and Trust Act (DATA) of 2011, H.R. 1841, 112th Cong. §§ 2(a)(1), 3(d)(3), 3(f)(2)(B), 4 (2011).

of clarity as to reasonableness may benefit from such approaches as well.

CONCLUSION

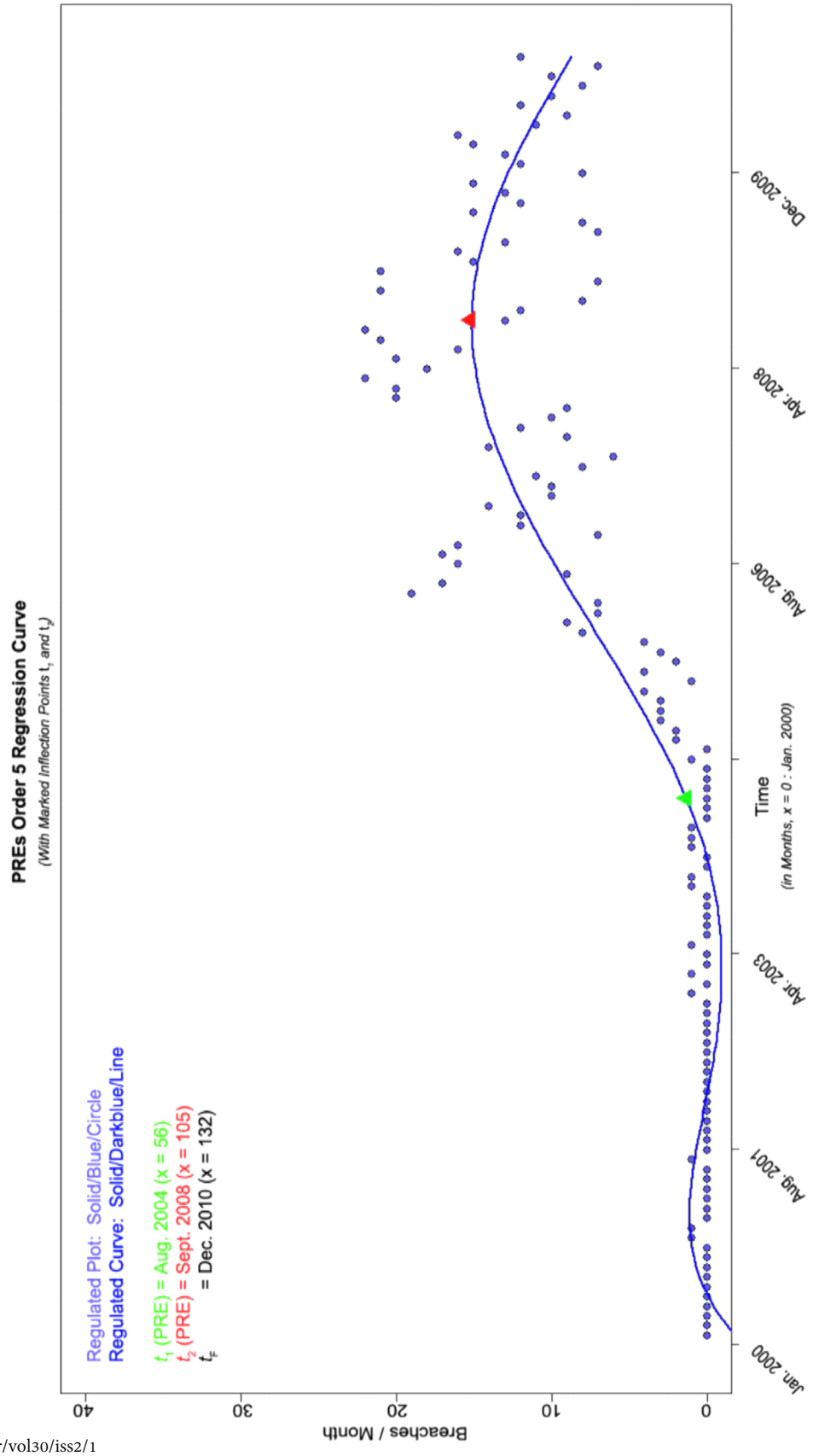
Three important conclusions follow from this Article. First, blended regulation—a mixture of Management-Based Regulatory Delegation and directive regulation—is superior at driving firms to implement information security practices that will prevent security breaches than is either regulatory model alone. This is a particularly important finding for regulators, both domestically and internationally. Domestically, since conducting the CISO interviews, we have seen the implementation of a breach notification requirement by the Department of Health and Human Services and guidance promulgated by the Securities and Exchange Commission that publicly-traded companies disclose material information about security risks to investors.[336] Internationally, the European Union has begun to consider breach notification requirements as well.[337] Massachusetts promulgated regulations in 2010 that bear some resemblance to the Management-Based Regulatory Delegation models found in HIPAA, GLBA, and the FTC's enforcement, and other states and federal regulators in other industrial sectors may wish to do so as well.[338] Thus, in summary, legislators and regulators considering information security measures may wish to evaluate whether a comprehensive approach to information security regulation—as opposed to a piecemeal approach—is appropriate.

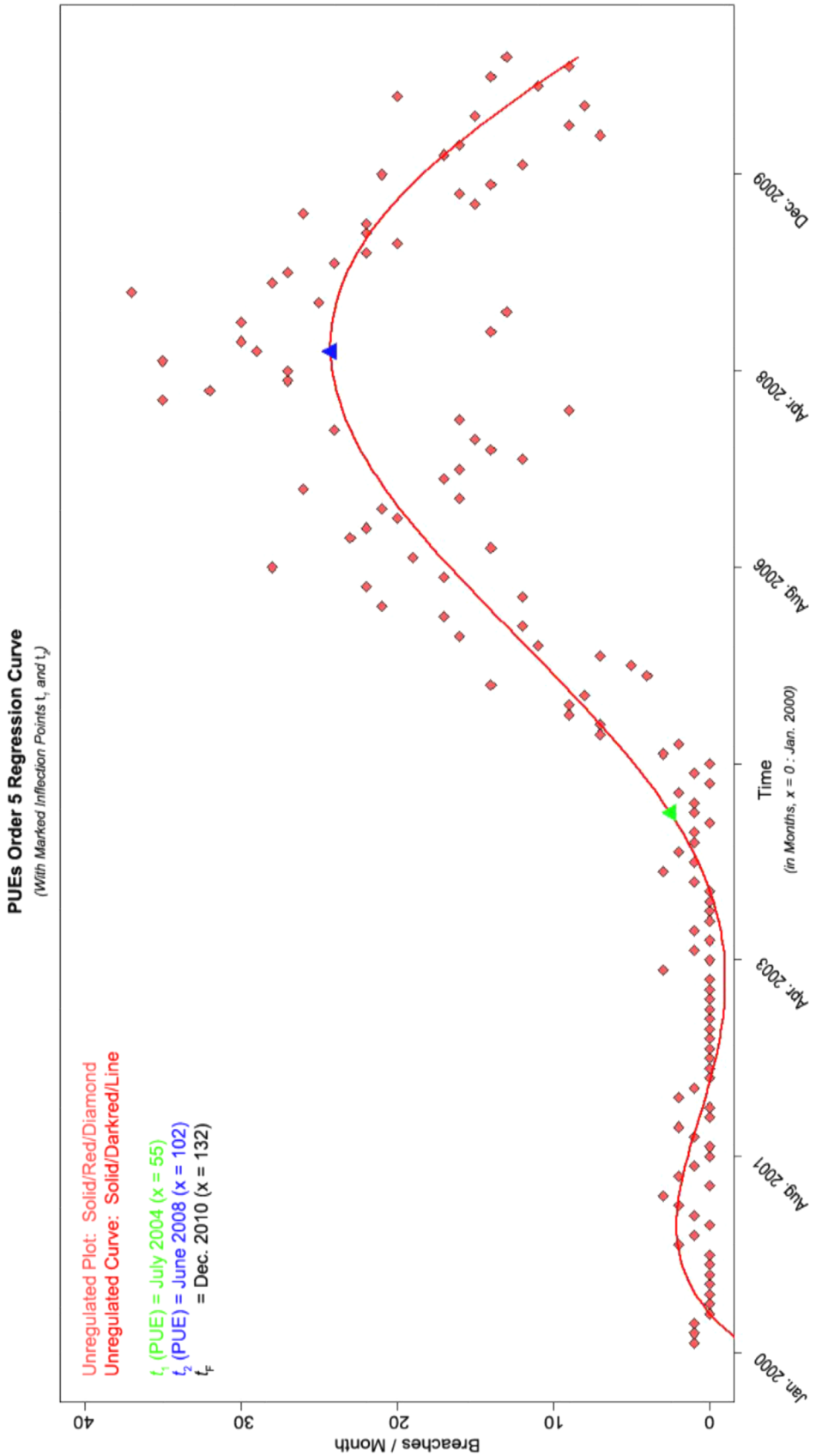
Second, the concept of Management-Based Regulatory Delegation—a deliberate choice by the legislature to heavily encode regulatory capture both in the administrative rulemaking process and in the compliance process—clearly affords advantages (efficacy at achieving the regulatory goal of preventing security breaches), but

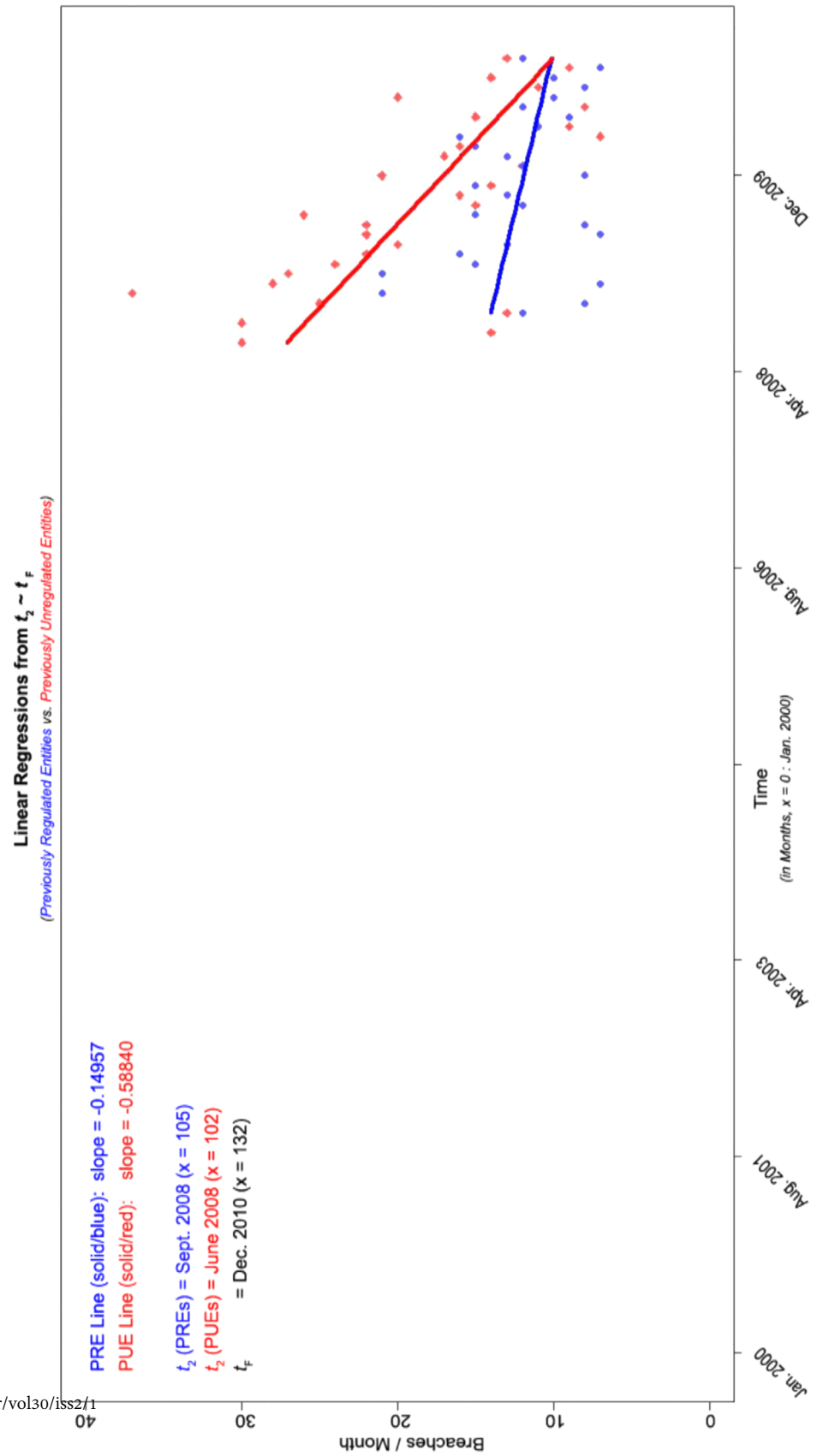
336. 45 C.F.R. pt. 160, pt. 164 (2013); *CF Disclosure Guidance*, *supra* note 294.
337. Commission Regulation 611/2013, 2013 O.J. (L. 173) 2.
338. 201 MASS. CODE REGS. 17.01 to -.05 (2010).

also incurs risk of a "race-to-the-bottom" in compliance standards. The preliminary data presented by the CISO interviews suggests that blended regulation, by layering on specific directive regulatory goals, may somewhat abate the risks of this deliberate regulatory capture. Further study of this concept certainly is warranted.

Finally, the use of information disclosure-based regulation to achieve the effect of directive legislation is an interesting concept. There is no evidence that when the California Legislature considered the first Security Breach Notification law, it envisioned an "encrypt everything" directive as the result. Yet that appears to have become the industry standard, at least for the foreseeable future. This "choice of compliance" approach to regulation may present regulators in other fields with an interesting option when heavy-handed traditional directive regulation is undesirable, but disclosure-based regulation where industries can "sort out for themselves the best approach" is more amenable.


PREs Order 5 Regression Curve
(With Marked Inflection Points t_1 and t_2)
Regulated Plot: Solid/Blue/Circle
Regulated Curve: Solid/Darkblue/Line
t_1 (PRE) = Aug. 2004 (x = 56)
t_2 (PRE) = Sept. 2008 (x = 105)
t_3 = Dec. 2010 (x = 132)
Breaches / Month
0
10
20
30
40
Jan. 2000
Aug. 2001
Apr. 2003
Aug. 2006
Apr. 2008
Dec. 2009
Time
(in Months, x = 0 : Jan. 2000)


PUEs Order 5 Regression Curve
(With Marked Inflection Points t1 and t2)
Unregulated Plot: Solid/Red/Diamond
Unregulated Curve: Solid/Darkred/Line
t1 (PUE) = July 2004 (x = 55)
t2 (PUE) = June 2008 (x = 102)
tF = Dec. 2010 (x = 132)
Breaches / Month
0
10
20
30
40
Jan. 2000
Aug. 2001
Apr. 2003
Aug. 2006
Apr. 2008
Dec. 2009
Time
(in Months, x = 0 : Jan. 2000)


Linear Regressions from $t_2 \sim t_F$
(Previously Regulated Entities vs. Previously Unregulated Entities)
PRE Line (solid/blue): slope = -0.14957
PUE Line (solid/red): slope = -0.58840
t_2 (PREs) = Sept. 2008 (x = 105)
t_2 (PUEs) = June 2008 (x = 102)
t_F = Dec. 2010 (x = 132)
Breaches / Month
0
10
20
30
40
Jan. 2000
Aug. 2001
Apr. 2003
Aug. 2006
Apr. 2008
Dec. 2009
Time
(in Months, x = 0 : Jan. 2000)