Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets

By

David Bernard Thaw

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Information Management and Systems

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Deirdre K. Mulligan, Chair
Professor Pamela Samuelson
Professor Todd LaPorte

Spring 2011

Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets

David Bernard Thaw

Abstract

Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets

by

David Bernard Thaw

Doctor of Philosophy in Information Management and Systems

University of California, Berkeley

Professor Deirdre K. Mulligan, Chair

Current scholarly understanding of information security regulation in the United States is limited. Several competing mechanisms exist, many of which are untested in the courts and before state regulators, and new mechanisms are being proposed on a regular basis. Perhaps of even greater concern, the pace at which technology and threats change far outpaces the abilities of even the most sophisticated regulators.

My Ph.D. dissertation focuses on understanding these laws – how we can classify them, what effects they have, and what are the implications of these effects for organizations and professionals. I explore these concepts through a mixed methods approach, utilizing both qualitative semi-structured interviews and quantitative data on breach incidence. The qualitative interviews inform the development of my hypothesis in addition to providing a basis for empirical analysis. The quantitative data is limited, but promising both in results and in the potential for the future analysis.

In this Dissertation, I report preliminary results as to the effect certain of certain laws on information security practices. I develop a system for classifying information security regulation, and develop hypotheses as to the effect certain types of regulation have on organizations and information security professionals.

Two notable conclusions result. First, the combination of Security Breach Notification (SBN) laws and management-based “regulatory delegation” models together is better at preventing breaches of personal information by organizations in the United States than is either model alone. Second, compliance-oriented prescriptive legislation such as SBNs weakens the role of security professionals within organizations, while management-based regulatory delegation models such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Financial Modernization Act (GLBA) strengthen the role of professionals within organizations.

This dissertation is dedicated to my father, Jack, who when I was six years old, handed me an inscribed book. Therein written were the words:

> "I hope you will read this book when you are older. It will tell you a lot about my work and also about my ideas and how I think about things. *When you read it, if it helps you think of new ideas of your own, then I will know that I wrote a good book.*"

Dad, I have carried that copy of your book with me my whole life. When you wrote it, few people were thinking about organizational behavioral as affecting the treatment of people with developmental disabilities. As I wrote this dissertation, I found that few people were studying the effect information security laws have on the structure of and manager-professional relationships within organizations.

You wrote a good book, Dad.

Table of Contents

Preface

When I first began my research into information security regulation, I was struck by the odd combination of a large volume of regulation on the books and a comparatively small amount of scholarly work studying the subject. As someone with a lifelong interest in information security, I am deeply concerned that policymakers make informed choices that ensure adequate protection of critical information and electronic infrastructure assets.

In my dissertation, I investigate the concept of information security regulation through an attempt to characterize, classify, and provide insight into understanding the nature, function, and implications of various regulatory approaches. I draw heavily upon empirical analysis – both qualitative and quantitative – in an effort to understand the function of law. While many of the results are preliminary, it is my hope that they provide a solid foundation both for the development of future scholarly work and for advising policymakers and key stakeholders about the character and function of information security regulation.

Acknowledgements

First and foremost, I offer special thanks to the members of my Qualifying Examination and Dissertation Committees, including Deirdre Mulligan (Chair of my Dissertation Committee), Pam Samuelson, Todd LaPorte, Yale Braunstein (Chair of my Qualifying Examination Committee), and John Chuang, for their mentorship, support, and patience with me through this process.

This material is based in part upon work supported by the Team for Research in Ubiquitous Secure Technology (TRUST), the Rose Foundation, and the Institute for Information Infrastructure Protection (I3P). Any opinions, findings, and conclusions or recommendations expressed in this material are solely those of the author and do not necessarily reflect the views of any of these organizations.

I would like to thank Aaron Burstein for his critical assistance in conducting the CISO interviews. I would also like to thank Jen King for her wonderful assistance, both administrative and substantive, in designing a process and protocol for conducting these qualitative interviews.

I would also like to thank Jack Balkin, Laura DeNaris, and the members of the Yale Information Society Project for providing me substantial feedback, support, and encouragement early in my writing process.

Finally, but most certainly not of least importance, I would like to thank my fellow School of Information doctoral students for their support, feedback, and advice over the years. The "Ph.D. lounge" in South Hall is a unique working environment that fostered intellectual development and exploration primarily as a function of the students who chose to work there each day. In particular, I would like to thank Joe Hall, Melissa Densmore, Jens Grossklags, Nathan Good, Paul Laskowski, Mahad Ibrahim, Danah Boyd, Jen King, Andrew Fiore, Yuri Takhteyev and Dilan Mahendran for their advice, mentorship, and encouragement over the years.

Acknowledgments for Chapter 2

I would like to thank Paul Mazzucco for the many hours he spent with me sorting through the concept of the Information Security Production Lifecycle. I would like to thank Elizabeth Khalil for her many hours of assistance and expert advice in analyzing financial regulatory issues. I would like to thank Mark Paulding for his mentorship and educating me about the practicalities of the various management-based forms of information security regulation. I would like to thank Tim Tobin for his mentorship and educating me about the practicalities of the security breach notification laws.

Acknowledgments for Chapter 3

I would like to thank the attendees of the 2010 Privacy Law Scholars Conference for their feedback on an initial draft of this work, in particular Gerard M. Stegmaier for his extensive feedback and for presenting my paper. I would like to thank Yale Braunstein and Ashok Agrawala for their assistance in developing the statistical methodology used to model breach incidence. I would like to thank Alexandra Zhang, Abhay Aneja, and Paul Mazzucco for their feedback on my implementations of these models.

Acknowledgements for Chapter 4

I would like to thank Todd LaPorte for the many hours spent in his office and on the phone thinking through issues of organizational structure. I would like to thank Deirdre Mulligan and Aaron Burstein for their assistance in framing the organizational structure questions and analyzing the CISO interview data.

Miscellaneous Acknowledgements

I would like to thank Mary Hodder for the many times she provided me a place to stay so I could return to Berkeley as frequently as I needed. Without question, I would not have been able to finish in time without her generosity. I would also like to thank Julian Park and Jenny Rosloff for contributing couches to my cause for the last two critical trips as I finished the final draft of this work.

I would like to thank Anthony Macchia for his support and encouragement over the years as I navigated the course of pursuing a Ph.D.

I would like to thank Jack Balkin, Laura DeNaris, Perry Fetterman, and the Yale Law School Information Society Project for providing me an academic home and a place to work while I was living in Connecticut.

I would like to thank Larry Davis, Ashok Agrawala, Brenda Chick, and the University of Maryland Department of Computer Science for providing me an academic home and a quiet place to finish my dissertation in the months before my appointment began at Maryland.

Finally, I would like to express my deepest gratitude to Deirdre Mulligan to her patience and encouragement as I faced many personal trials over the past four years. You did not give up on me, and gave me the chance I needed to be able to finish something of which I am very proud.

1 INTRODUCTION

The concept of information security is not new. As far back as the Roman Empire, Julius Caesar is credited with developing a basic substitution cipher known as the Caesar Cipher.[1] Mathematics and cryptology have advanced substantially over the roughly 2000 years since Caesar's time. Encryption schemes such as the Advanced Encryption Standard (AES)[2] now exist, and the United States National Security Agency's Central Security Service has certified AES as effective for protecting even information classified at the Top Secret level since its inception in 2001 through the present day.[3]

What has changed is the volume of information being handled electronically and the volume and types of information considered sensitive enough to warrant protection. Thirteen years ago, when I was a freshman at the University of Maryland, my Social Security Number was printed – in large text – on my student ID card (which I was required to present upon demand).[4] Today, many statutes regulate the usage, storage, and protection of Social Security Numbers in the United States.[5] Although perhaps obvious to most readers of this work, the volume of digital information available has increased – quite literally – exponentially in recent years. According to a February 2011 Washington Post article, researchers from the University of Southern California estimated that from 1986 to 2007 the world's volume of digital data grew from about 20 million gigabytes to (or $2 * 10^{16}$ bytes) to 276.12 exabytes (or $2.7612 * 10^{20}$ bytes).[6] That's about *one million times* more information.

Sensitive information means different things to different people, and certainly has different meanings across cultural and national boundaries. In the consumer protection context, it often refers to information describing individuals or information that may be used to compromise an individual's privacy, identity, or finances. From the perspective of the organization, it may include information such as trade secrets, scientific advances for which the organization has not yet sought patents, or "insider" information relating to

[1] *See* Caesar Cipher, WIKIPEDIA, http://en.wikipedia.org/wiki/Caesar_cipher (citing Edgar C. Reinke, *Classical Cryptography*, 58 THE CLASSICAL J. 114 (Dec. 1992)).

[2] *See* Advanced Encryption Standard, FED. INFO. PROCESSING STDS. PUB. 197 (Nov. 26, 2001) *available at* http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[3] *See* NSA Suite B Cryptography, http://www.nsa.gov/ia/programs/suiteb_cryptography/ (last visited Apr. 13, 2011).

[4] The University of Maryland has since changed their practices in this regard, both discontinuing the printing of SSN's on student ID cards and replacing student ID numbers with identifiers not tied to an individual's Social Security Number. The Student ID card in question was destroyed when I had it replaced after the magnetic strip malfunctioned, and the replacement card did not have my SSN printed on it (hence why I do not have an image available to this effect).

[5] *See, e.g.,* CONN. GEN. STAT. §§ 42-470, 42-471.

[6] Brian Vastag, *Digital Data Now Come in Exabytes*, WASH. POST, Feb. 11, 2011, at A3.

the organization’s financial situation. Despite these differences, one thing is certain – whatever the definition of sensitive information, individuals, organizations, and governments are becoming increasingly concerned with its protection. It is this concern that formed the foundation of my research. Since vast amounts of potentially sensitive information are held by private organizations, it is important to understand what drives those organizations to protect their information assets.

Current information security law in the United States focuses heavily on the consumer protection aspects discussed above. I describe the key components of this information security regulatory landscape in Chapter 2: Classifying Information Security Law and Regulation. Current information security law and regulation focuses on protecting specific types of information, such as Social Security Numbers, financial account information, and health information, rather than upon the general “health” and “security” of information and control networks. To the extent these laws and regulations require general security measures, such measures are in furtherance of protecting this consumer information, rather than with the goal of protecting the network itself.

This dissertation examines how law and regulation affect the information security practices of large organizations in the United States. Through a combination of quantitative and qualitative methods, I endeavor to address three questions: 1) how can we classify information security laws to understand their function; 2) what types of effects did information security laws have on organizations’ security practices; and 3) what implications the function of these laws have for the structure of and professional relationships within organizations. I have organized this work into three substantive chapters – Chapter 2: Classifying Information Security Law and Regulation, which addresses question 1; Chapter 3: The Relationship Between Regulatory Models and Information Security Practices, which addresses question 2; and Chapter 4: The Differential Effects of Information Security Regulation on Professionalism in Large Organizations, which addresses question 3.

2 CLASSIFYING INFORMATION SECURITY LAW AND REGULATION

2.1 *INTRODUCTION*

The goal of this Chapter is to develop a system for classifying information security laws and regulations according to their functional character to use in evaluating how and why they alter information security practices at regulated organizations.

To develop a system of classification I begin by examining existing work in this area. The work of two authors, Cary Coglianese and David Lazer, is particularly informative as they have made substantial efforts to develop a typology for classifying regulatory systems with a particular focus on what they call "management-based regulation." Management-based regulation, as I illustrate in this Chapter, is the functional character of many of the key information security laws and regulations in place today and identified as influential by the Chief Information Security Officers ("CISOs") I interviewed.

Building upon Coglianese and Lazer's work, I investigate the aspects of what I describe as the Information Security Production Lifecycle ("ISPL"), that process which describes the cycle from definition of an information security goal, through design, implementation, and evaluation of means to achieve that goal, to outcomes indicating the efficacy of those means to achieve that goal. Using this timeline, I identify shortcomings in Coglianese and Lazer's framework as it applies to existing and potential information security regulations. I then propose a revised framework which allows for more precise and accurate characterization of current information security regulations.

I proceed to classify current information security laws and regulations identified by the CISO respondents as key in driving their information security practices, and include other regulatory structures that have substantial import in the overall framework of information security regulation. Later, in Chapters 3 and 4, I use these classifications and draw upon the CISO interview data to examine hypotheses about how various forms of regulation will differentially affect information security practices in organizations (Chapter 3) and differentially affect the relationships between senior managers and professionals within organizations (Chapter 4).

2.2 *HYPOTHESES*

I propose hypotheses about the four major components of information security regulation in the United States: 1) Security Breach Notification Laws ("SBNs"); 2) the Health Insurance Portability and Accountability Act's ("HIPAA") Security Rule; 3) the Gramm-

Leach-Bliley Financial Modernization Act's ("GLBA") Safeguards Rule and Interagency Guidelines on Information Security; and 4) the Federal Trade Commission's ("FTC") jurisprudence with respect to its data security enforcement actions. These hypotheses discuss the classification of each of those regulatory frameworks according to the revised typology I propose in Section 2.6.

> **Hypothesis H1: Security Breach Notification Laws are a mixture of performance-based regulation targeting the output/efficacy stage of the ISPL and means-based regulation affecting the design/planning and implementation/maintenance stages of the ISPL.**

I discuss and evaluate Hypothesis **H1** in Section 2.7.1 below.

> **Hypothesis H2: The HIPAA Security Rule is a hybrid form of management-based regulation targeting each of the design/planning and the implementation/maintenance stages of the ISPL.**

I discuss and evaluate Hypothesis **H2** in Section 2.7.2 below.

> **Hypothesis H3a: The FTC's GLBA Safeguards Rule is a hybrid form of management-based regulation targeting each of the design/planning and output/efficacy stages of the ISPL.**

> **Hypothesis H3b: The GLBA Interagency Guidelines on Information Security are a hybrid form of management-based regulation targeting each of the design/planning and the implementation/maintenance stages of the ISPL.**

I divide Hypothesis **H3** into two separate sub-hypotheses since the two primary sets of regulations promulgated pursuant to GLBA vary in how they target the ISPL. I discuss and evaluate Hypotheses **H3a** and **H3b** in Section 2.7.3 below.

> **Hypothesis H4a: FTC enforcement actions are a hybrid form of management-based regulation targeting each of the design/planning and the output/efficacy stages of the ISPL.**

> **Hypothesis H4b: FTC enforcement actions are a hybrid form of means-based regulation targeting each of the design/planning and implementation/maintenance stages of the ISPL.**

> **Hypothesis H4c: FTC enforcement actions are a hybrid form of means-based regulation affecting all of the design/planning, the implementation/maintenance, and the output/efficacy stages of the ISPL.**

I divide Hypothesis **H4** into three separate sub-hypotheses to address what I propose as three different effects of the FTC's enforcement action jurisprudence: 1) direct management-based effects on the subject of the enforcement action; 2) direct means-based effects on the subject of the enforcement actions; and 3) indirect means-based effects that appear to apply to other entities who were *not* the subject of the enforcement action, even in the absence of formal regulations promulgated to such effect. I discuss and evaluate Hypotheses **H4a**, **H4b**, and **H4c** in Section 2.7.4 below.

2.3 REGULATORY FRAMEWORKS

Information security laws have not yet been classified in the literature on regulation. Doing so is important not only as an effort unto itself, but also to addressing the specific hypotheses examined in this paper. This section examines a framework developed by Cary Coglianese and David Lazer (C&L) for characterizing forms of industrial regulation. I present an overview of Coglianese and Lazer's typology, and then discuss its applicability to information security regulation. Specifically, I consider timing issues – C&L's typology strictly links each type of regulation to one point in the industrial production cycle. I identify examples in information security regulation where the type and timing of regulation do not match the pairings proposed by C&L. I also identify other issues raised by examples where C&L's typology does not match well with specific information security regulation or potential regulation.

2.3.1 Coglianese and Lazer (2003)

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.[7] They suggest that intervention may occur when planning production ("planning stage"), implementing production ("acting stage"), or determining the final outputs of production ("output stage"). Each of these stages, according to the C&L's model, corresponds to a different type of regulation. The sections that follow discuss these stages in detail.

2.3.1.1 Technology-based Regulation

As defined by Coglianese and Lazer, technology-based regulation is an approach in which regulatory standards govern the means of production. Occurring at the implementation (or "acting") stage, it specifies technologies that must be employed or

[7] Cary Coglianese and David Lazer, Management-Based Regulation: Prescribing Private Management to Achieve Public Goals, 37 LAW & SOCIETY REV. 691, 693-94 (Dec. 2003).

processes that must be followed.[8] 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 measures such as anti-virus and anti-malware software on their systems.

2.3.1.2 Performance-Based Regulation

Performance-based regulation is an approach in which regulatory standards govern the final state or result of a production process.[9] 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.

2.3.1.3 Management-Based Regulation

Management-based regulation is an approach in which regulatory standards address conditions that must be met during the planning stage of a productive process – i.e., before manufacture of a product or provision of a service begins.[10] It most commonly requires organizations to conduct risk assessments and/or produce risk management plans.[11] 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

[8] *Id*. at 694.

[9] *Id*.

[10] *Id*. at 694-96.

[11] As noted by Coglianese and Lazer, management-based regulation may also require organizations to implement and adhere to the risk management plans they develop. 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 which much be achieved. The specifications of these technology and performance requirements will obviously differ as the organizations self-define the guidelines. *See Id*. at 707-711.

address. The "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 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.

2.4 *TIMING IN THE COGLIANESE AND LAZER TYPOLOGY AND INFORMATION SECURITY PRODUCTION*

C&L's typology is heavily depending on the "timing" of regulation. They "distinguish between different types of regulatory instruments based on the organizational stage that each instrument targets."[12] Considering timing as a key component of classification is informative. The strict one-to-one linkages between types of regulation and points-in-time cannot adequately describe certain information security regulatory models currently in place. This section details examples of regulatory models where the method of regulation and its "timing" within the production lifecycle do not match C&L's typology.

2.4.1 The Role of "Timing"

To understand the ways in which C&L's typology overlooks certain types (and potential types)[13] of information security regulation, it is first necessary to understand what constitutes a security "good" or "output." C&L define outputs in the context of traditional industrial production.[14] 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)."[15]

[12] Coglianese and Lazer at 694.

[13] Discussing "potential types" of information security regulation is critical at this juncture both because there 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. *See, e.g.,* S. ___, the Commercial Privacy Bill of Rights Act of 2011, 112th Cong. (draft text 2011) *available at* http://kerry.senate.gov/imo/media/doc/Commercial%20Privacy%20Bill%20of%20Rights%20Text.pdf.

[14] Coglianese and Lazer at 693.

[15] *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. 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,[16] is an exercise in risk mitigation, not risk prevention. Thus many of the deliverable "goods" or "services" are defined by engaging in activities that are likely, but not guaranteed, to mitigate system compromise. It is therefore the act of engaging in those activities, *not* the result of the activities themselves, that constitutes the output for information security. As noted below, 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. C&L consider three industrial activities as examples in discussing their typology: food safety, pollution, and industrial safety.[17] 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.[18] Unlike these three categories, however, information security lacks well-defined metrics by which to evaluate outcomes.[19] The lack of well-defined metrics makes it difficult to evaluate information security outcomes strictly at the output stage. Professionals[20] and regulators[21] 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."[22]

[16] 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."

[17] *See id*. at 696-700 (discussing these three examples in the context of C&L's typology).

[18] Information security is, in large part, a process/procedure/goal (to protect assets) associated with some other productive activity.

[19] Several of the CISO respondents lamented the lack of available metrics particularly as it pertained to justifying information security expenditures to management.

[20] *See, e.g.,* Section 4.1.1.1.

[21] *See, e.g.,* Sections 2.7.2, 2.7.3, and 2.7.4 discussing how HIPAA regulators, GLBA regulators, and the FTC (generally) evaluate information security efficacy in the context of their promulgated regulations and enforcement actions.

[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."

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 C&L'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[23] 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 C&L's typology. As indicated below in Section 2.4.2.3, the refinements I propose address this disconnect by redefining the final stage of production to include outputs that occur 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. As explained here, understanding the role of timing is critical to understanding the shortcomings of C&L'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 C&L's typology.

2.4.2 The Information Security Production Lifecycle ("ISPL")

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

[23] As different 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.

"botnet," 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 recognized information security goal, or "product," independent of the organization's specific focus on countering a particular or general threat of machine hijack.[24]

In the following three sections, I propose a friendly refinement to the stages of production examined by C&L. The purpose of this refinement (and renaming) is specific to information security and to industries that may resemble its production characteristics.[25]

2.4.2.1 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.[26] As discussed in this section, 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[27] do require that such decisions be made at the planning stage. 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."[28]

[24] CISSP Bulletin at 12 (noting "[preventing] or resond[ing] to attacks (e.g., malicious code, zero-day exploit, denial of service)" and "implement[ing] and support[ing] patch and vulnerability management" as "Key Areas of Knowledge" in the "Operations Security" domain (*see* Chapter 3, Section 3.4.7)).

[25] The following should not be interpreted to suggest that the stages of production examined by C&L 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.

[26] Coglianese and Lazer at 693-94.

[27] *See, e.g.*, Standards for the Protection of Personal Information of Residents of the Commonwealth ("Mass. Data Security Standards"), 201 MASS. CODE REGS. 17.00.

[28] Coglianese and Lazer at 702 (discussing how management-based regulation mandates *that* firms engage in planning activities but does *not* specify how those activities must implement mechanisms to achieve regulatory goals).

2.4.2.2 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. In their typology, it is that stage at which technology-based regulation is targeted.[29]

2.4.2.3 Efficacy/Output Stage

The efficacy/output stage is that portion of the ISPL encompassing definable outcomes. As discussed above in Section 2.4.1, 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 defined in Section 2.4.1 as steps taken to mitigate risk; and 2) *measurable* outcomes, or those for which an external metric[30] can evaluate success. Together, these two categories define the efficacy/output stage.

This is markedly different from C&L'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.[31] As noted above in Section 2.4.2, outputs in traditional industries come into being at the end of a production cycle as the result of some process or steps designed to 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 (discussed in Section 2.4.2 above), 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

[29] Coglianese and Lazer at 693-94.

[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 in Section 2.4.1, exist at all stages of the ISPL.

[31] Coglianese and Lazer at 693-94.

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 thus a necessary refinement to C&L'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.[32] These types of occurrences always are 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.

2.5 SHORTCOMINGS IN THE COGLIANESE AND LAZER TYPOLOGY AS APPLIED TO INFORMATION SECURITY REGULATION

The preceding sections lay a foundation for understanding the differences between production in information security and production in more traditional industries. Using this foundation, I proceed to identify shortcomings in C&L's typology as it applies to information security. I proceed through their three categories, discussing specific shortcomings of each and identifying existing (and potential)[33] types of information security regulation that cannot properly be characterized by C&L's typology.

2.5.1 Technology-Based Regulation is Underinclusive

As discussed above (Section 2.3.1.1), C&L's typology strictly links technology-based regulation to the "acting" stage of the industrial production cycle. This approach generally is underinclusive, ignoring regulatory instruments that address methods and means but do so at a different stage of the production cycle.

Consider the case, discussed above in general terms, of where the technology is itself the output of the productive process. If the "good" in question is an authentication

[32] The concepts of measurable (negative) security incidents involving system compromise are more thoroughly examined in Chapter 1, Section 3.6.
[33] *See* supra n. 13.

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 – as identified by the International Information Systems Security Certification Consortium (ISC)^2, security considerations must be a part of the software development life cycle.[34] However, to limit the term "technology-based regulation" only to those events occurring during production is misleading in this context.

2.5.2 Performance-Based Regulation Fails to Consider Effects at the Acting Stage

The term "performance-based regulation" is descriptive in the context of information security regulation. Like other subjects of regulation, information security has output characteristics than can be identified and, in many cases, quantified. Interestingly, however, the practical effect of certain types of performance-based information security regulations – most notably security breach notification laws[35] – has been to drive compliance activities at the *production* stage, rather than at the output stage. A striking example of this phenomenon in the SBN context is the rapid adoption in recent years of technologies to encrypt "personal information" as defined under SBNs. This adoption appears to result, in large part, from provisions in most jurisdictions' SBN statutes providing "safe harbors" from notification requirements if the compromised or lost data was encrypted.[36]

The result is a situation in which a regulation addressing an output condition – the unauthorized access of personal information – ends up driving a production condition – the method of securing personal information. This type of situation suggests that, at least in the information security context, a complete framework should consider both the intended function of the regulation (as written) and what effects the preferred method of compliance may have. The present example suggests that these two conditions may diverge across stages in the ISPL. In the case of SBNs, for example, they target an output/efficacy condition (reduction of compromised personal data and/or reduction of breach incidence generally) but specify, or at least result in, a preferred compliance method at the implementation/maintenance stage (encryption of all data subject to the regulation).

[34] *See* CISSP Bulletin at 4 (noting that "security of the application environment," including "certification and accreditation" and "auditing and logging" are essential components of "security in the system life cycle.").
[35] *See* Section 2.7.1.
[36] *See* Chapter 2, Section 3.9.4.3.

2.5.3 Management-Based Regulation Fails to Consider Hybrid Models

As discussed above in Section 2.3.1.3, C&L's typology ties management-based regulation to the planning stage of production. Unlike with technology-based or production based regulation, C&L'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.[37] 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.[38]

Enforcement such as that by the Federal Trade Commission however, as discussed in greater detail in Section 2.7.4, presents a hybrid model of management-based regulation not captured by C&L's typology. FTC enforcement actions result both in specific compliance orders and in a requirement to conduct regular information security (and/or privacy) assessments. Unlike the assessments conceived under traditional management-based regulation, FTC-ordered assessments are *reactive* in nature instead of *proactive*. Furthermore, the effective goals of those assessments are tied *ex ante* (the assessment) to those specific compliance objectives.

The effective result is a hybrid style of management-based regulation involving assessments beginning from a different point than C&L'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.[39]

2.6 A REVISED FRAMEWORK SUITABLE TO INFORMATION SECURITY REGULATION

In the preceding sections, I identify shortcomings with C&L's typology as it applies to information security regulation. To address these issues, I propose a faceted classification system[40] comprising a matrix based on four elements: 1) the characteristic "type" of regulation; 2) what time in the ISPL the regulation targets/affects; 3) whether the regulatory aspect being examined is an explicit target or a secondary (or unintended) effect; and 4) the extent (if any) to which private parties may be involved in the

[37] *See* Coglianese and Lazer at 706.
[38] *See* Section 2.7.2.
[39] *See* Section 2.7.4.4 for a further discussion of this phenomenon.
[40] *See infra* Section 2.6.3 ("Tagging" Using a Faceted Classification System) which provides a more comprehensive discussion of this type of classification system.

rulemaking process.[41] This classification system will not be unitary but rather will allow for regulation to have more than one "category" attributed to it. The resultant classification will thus be a function of what combinations of categories apply to each statute, regulation, or other regulatory device. The framework therefore comprises "classifications", more than one of which can be applied to a regulation, where each classification comprises four descriptors (one from each of the categories above).

Information security regulations often produce regulatory outcomes at stages in the production cycle other than – and sometimes even instead of – those targeted by the regulation. This disconnect between "target" and "effect" relates to the rapidly-changing technical complexity of the subject matter being regulated. Thus it is important to include a chronological element in any framework designed to characterize information security regulation.

2.6.1 Developing the Classification System – Translating Shortcomings to Refinements

As discussed here and above in my analysis of Coglianese and Lazer's model,[42] this aspect of the information security production lifecycle suggests that a chronological, as opposed to purely characteristic, approach should be employed to analyze the effect of information security regulation. For example, such a framework for analysis must conceive of regulations designed to govern information security goals – described above as "performance-based regulation" – but that address elements occurring at the design or production stages of the lifecycle. To accomplish this goal, as described above, I propose augmenting the C&L framework by decoupling their characteristic "types" of regulation (management-based, technology-based, production-based) from the three points in the production lifecycle each type regulation may effect. Each regulation (or aspect thereof) is then categorized by its characteristic type and the point in the production lifecycle it targets or that point which it produces a secondary or unintended effect. This latter distinction is captured in a third parameter which describes whether the regulation (or aspect thereof) being considered is in fact a "target" (generally meaning the regulation's language or formal interpretation suggests the intent to act on a certain stage in the production lifecycle, regardless of whether it is successful in doing so) or an "effect" (generally meaning the regulation, in practice, produces an empirically observable change

[41] As demonstrated later in this Chapter, the regulations I examined generally all share exactly one classification according to the fourth parameter. While not exclusive of the concept of applying multiple tags with different values for Parameter 4, the present analysis considers only one such application and thus the tags discussed throughout this chapter are often presented only with the first three parameters when more than one tag is applicable to a law or regulation. Section 2.7 identifies the Parameter 4 values for each law or regulation considered in this paper.
[42] *See supra* Section 2.3.

in behavior at the given point in the production lifecycle). Finally, each regulation is characterized, as discussed in Section 2.6.3.4, by whether the legislation is prescriptive, involves traditional rulemaking, or involves the "regulatory delegation" style of rulemaking which specifically requires the involvement of private industry stakeholders.

In the subsections that follow, I provide examples of specific regulations (or potential regulations[43]) not captured by C&L's model and discuss how those exceptions suggest employing the faceted classification system I propose above.

2.6.1.1 Example 1: Secure Access Control Requirements – Regulation Targeting More Than One Stage of the ISPL

One shortcoming of C&L's typology is that it considers most regulation[44] to target exactly one stage of production. Many information security regulations, however, target more than one stage of the ISPL. Consider, for example, a regulation that mandates secure access control, including the use of identification and passwords that are not vendor defaults.[45] Such a regulation requires certain activities to occur at the design and planning stage (e.g., development of a secure access control system), but also specifies certain details about how the results of those activities must be implemented and maintained (e.g., that passwords must not be vendor defaults).[46] Thus C&L's apparently mutually exclusive system of categorization does not provide a complete framework for classifying such information security laws and regulations.

To provide a complete framework, therefore, a system of categorization must conceive of categories not by selecting certain combinations of attributes and creating categories from those combinations, but rather creating a faceted classification system for "tagging" laws and regulations with attributes. While each law or regulation ordinarily will be described by one set of four parameters – e.g., "1) technology-based regulation; 2) targeted at; 3)

[43] *See* supra n. 13.

[44] As discussed above in Section 2.3.1.3, C&L recognize a limited exception to this "single-target" concept for management-based regulation. However, this single exception is insufficient to address the issues raised in the present section.

[45] *See* 201 MASS. CODE REGS. 17.04(2).

[46] An alternative approach to thinking about this distinction would be to separate those elements of the regulations pertaining to planning from those pertaining to implementation. Such an approach, however, seems unsuited to the information security context in which design, implementation, and result are inexorably intertwined. It is not the case, for example, that the application of an alternative security technique can "make up for" a failure to implement secure authentication mechanisms. This path-dependence differs from other types of regulation Coglianese and Lazer study, such as food safety, in which the risks associated with a failure to engage in "poke and sniff" tests at one stage in the meat and poultry production process could be mitigated by application of tests for bacterial or other anti-microbial techniques later in the production process.

the output/efficacy stage; 4) that is prescriptive legislation") – more than one such description can be applied to a law or regulation. Under such a system, therefore, regulations are categorized not by placing them into a singular element in a framework, but by allowing them to be tagged with multiple descriptors. In the example above, the excerpt from the Mass. Data Security Standards would be tagged both as technology-based regulation targeting the Design/Planning stage and as technology-based regulation targeting the Implementation/Maintenance stage. Both examples, as discussed in Section 2.7.5.1, are a form of traditional notice-and-comment rulemaking. What descriptors would apply with respect to the effects of the regulation would need to be determined by empirical observation.[47] The CISO interviews provide empirical evidence for classifying some of the current information security laws and regulations. In Section 4.2 I suggest future research that may further inform these classifications.

2.6.1.2 Example 2: Technological Countermeasures as an Outcome – Regulation Affecting Technology But Not Targeted at the Implementation/Maintenance ("Acting") Stage of the Production Lifecycle

As discussed above in Section 2.3.1.1, Coglianese and Lazer's definition of technology-based regulation is underinclusive. First, it fails to account for instances where the target of the regulation is either an output condition or a planning or design requirement, but where the method of regulation requires the implementation of specific technologies or practices. Consider the example suggested above, where a regulation specifies that custodians of sensitive personal information must employ security measures such as anti-virus and anti-malware software on their information systems.[48] To be sure, the use of such systems involves regulating technology. Such a requirement may be designed to "require firms to adopt [these technologies] to promote social goals,"[49] such as a more secure overall environment for information exchange. Such a requirement, however, is a goal unto itself as the more systems that employ these technologies, the more effective the technology becomes at combating the spread of threats. Section 2.4.2 discusses this concept in more detail, and the conclusions to Chapter 3 (Section 3.11) identify that, in fact, organizations applying good general security principles appear to have greater capacity to address subsequent specific security principles not previously addressed in the

[47] In the context of this example, drawn (as identified *supra* in note 45) from the Mass. Data Security Standards, empirical observations as to the effects of this regulation are outside the scope of the present research. This research began in 2007, and was concluded well before the March 1, 2010 effective date of the Mass. Data Security Standards.

[48] *See, e.g.,* 201 CODE MASS. REGS. 17.04(7) (requiring that ". . . a security system covering [a regulated entity's] computers . . . shall have . . . [r]easonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis").

[49] Coglianese and Lazer at 701.

general regulation. A similar type of analysis is true with encryption technologies – the more systems that employ secure (encrypted) communications channels, the greater the overall percentage of communications involving a given system will be encrypted.[50] As noted above, while the distinctions between these outcome-oriented regulations and process-oriented regulations may appear overly fine, they are important to characterizing the functional distinctions among various approaches to regulating information security. I predict these distinctions will become even more common as utility systems and other large networked environments become the subject of information security regulation as a whole. In those cases, regulations mandating network-wide system security software or encryption will be critical to mitigating the risk of negative externalities and will become (as discussed in Section 2.4.2) the goal "outcomes" themselves.

Admittedly, in the context of current regulation, such as the Mass. Data Security Standards, the anti-virus/anti-malware example may be more a theoretical consideration than a practical one, as the facial intent of the statute appears to be protection of specific data rather than increasing the efficacy of such security technologies. We have not yet reached the point, described above, where system-wide protection is considered sufficiently important to mandate the use of system security software as an outcome unto itself. The email example, however, while not the subject of a current regulation, is likely to become the subject of increased scrutiny as the use of email becomes more pervasive globally. Currently several forms of sensitive information, including privileged attorney-client information,[51] are permissible for transmission via email in many U.S.

[50] These generalized statements refer to the consideration of applications in practical use, where mixed (secure/unsecured) communication channels are necessary as not all systems involved can be forced to employ encryption. A well-known example is the public email system, for which there are various encryption solutions available but for which both 1) there is currently no effective way to mandate that a single – or even any qualifying – encryption mechanism be employed by all systems using public Internet-based email; and 2) effective operation of the system requires that all public-facing email accounts be able to send and receive from all other public-facing accounts regardless of whether they support a compatible standard for message encryption. I stress that the constraints outlined above are *both practical and technical*, and it is the combination of these two categories of constraints that creates the problem.

[51] *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999) ("a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet"). *See also* N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 820 (2008) ("[a] lawyer may use an e-mail service provider that conducts computer scans of e-mails to generate computer advertising, where the e-mails are not reviewed by or provided to other individuals").

jurisdictions.[52] While such an approach has, to my knowledge, not yet produced any serious security incidents, the increasing sophistication of attackers and the financial value of identities and corporate secrets[53] suggest the increasing likelihood of such incidents. Accordingly, the likelihood of regulation in this space will increase. Given these conditions, it seems appropriate to consider this structure of regulation – technology-based regulation occurring at the efficacy/output stage, rather than the implementation/maintenance stage – as one that needs to be addressed by any complete framework for classifying information security regulation.

2.6.1.3 Example 3: HIPAA "Workforce Security" Provisions – Regulation Not Affecting Technology But Targeted at the Implementation/Maintenance ("Acting") Stage of the ISPL

Some information security regulations affect the means of production (i.e., are targeted at the implementation/maintenance stage) and do not regulate technology. In considering such cases, a broad interpretation of the term "technology" is informative. Such a broad definition allows for certain administrative and physical security requirements to fit C&L's definition of "specific technologies or methods." Nonetheless, there still remain certain regulations that do not fit this definition yet target the implementation/maintenance stage of the ISPL. While it may be possible to consider such regulations, in part, as management-based regulation,[54] such a description does not seem complete for regulations with an apparent intent to regulate means.

Consider the following regulations promulgated by the Department of Health and Human Services pursuant to its authority under the Security and Privacy Rules of the Health Insurance Portability and Accountability Act (HIPAA) in 45 C.F.R. § 164.308(a):[55]

[52] The author is aware that the analysis done by some of these regulating authorities is (at least) no longer consistent with the practice realities of the Internet. It is, for example, facially unreasonable to assume that unencrypted email messages, handled by multiple private entities, are as unlikely to be intercepted by a third-party as are those handled by a government corporation and only by government employees (or their designees). Furthermore, the public Internet email system differs substantially from postal mail in that "opening" an email message for reading may not leave forensic evidence (different from that evidence normally left when the message is passed along during normal IP routing) thereof, whereas the opening of a physically-sealed envelope is almost certainly likely to leave forensic evidence. Further discussion of these issues is outside the score of this research; they are identified here to provide context for the purpose of the asserted proposition that regulation in this space is possible, perhaps even likely.

[53] *See* Chapter 3, Section 3.2.3 discussing a 2010 Forrester Research report covering, among other things, the value corporations self-identified for their information assets.

[54] *See* Section 2.3.1.3 above for a discussion of how management-based regulation does consider (limited) effects at the "acting" stage of C&L's typology.

[55] 45 C.F.R. § 164.308(a)(3)(i) – (3)(ii).

> (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
>
> (ii) Implementation specifications:
>
> (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
>
> (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
>
> (C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

These regulations describe administrative security requirements for organizations ("covered entities") subject to the jurisdiction of the HIPAA Security and Privacy Rules. Certainly, none of them discuss any specific technologies. While the regulations do specify *that* methods to accomplish tasks must be employed, they do not specify which specific methods must be employed. In §164.308(a)(3)(ii)(C), for example, the regulations require that covered entities implement procedures to ensure that employee access to protected health information (PHI) is terminated when they no longer are employed by the organization or when access is no longer appropriate (as a function of their job responsibilities). There are a variety of technical and administrative methods to accomplish this goal. To describe this regulation as requiring any one specific technology or method would characterize the regulation differently than its (apparent) intended effect. In this respect, C&L's technology-based regulation does not adequately describe this regulation. Likewise, management-based regulation does not adequately describe this regulation because its intent is more than just to require the development (and even adherence to) a plan. The regulation, in fact, does not even "require firms to engage in [any] planning [activities],"[56] the central element of management-based regulation under C&L's typology. Thus in this example neither technology-based regulation nor management-based regulation fully describes this regulation.

As specified in 45 C.F.R. § 164.308, a "covered entity" must implement policies and procedures consistent with the specifications above and with the general specifications of

[56] Coglianese and Lazer at 706.

§ 164.306. § 164.306 states generally that compliance with these regulations shall be appropriate to the "size, complexity, and capabilities"[57] of the organization (unless otherwise specified) and that those regulations designated as "Addressable" may be considered by the entity as to whether or not the regulations are appropriate given these factors.[58] Moreover, the language specifically provides for a "flexibility of approach" stating that "[c]overed entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart."[59]

While the regulations excerpted above might, in their strictest sense, be considered to require that firms adopt technologies or methods, given the extensive flexibility language afforded to covered entities it seems unlikely that these regulations would, on their face, require organizations to implement any one particular technology.[60] These regulations do, however, clearly target decisions organizations make at what C&L refer to as the "acting" stage. Thus they represent an example of regulation targeting the implementation/maintenance stage of the ISPL that does not specify which technologies or methods are acceptable for use, but rather the goals those technologies or methods must accomplish. However, as different from performance-based regulation, the regulations discussed here neither specify performance levels nor (as discussed above) target outputs.

In the context of information security, the distinction between a requirement to implement a specific technology and that to implement any technology capable of achieving a goal is substantial. It is important that any framework for characterizing information security laws account for these subtleties if the framework is to have predictive value for informing future policymaking. Thus any such framework must account for regulation that targets the implementation/maintenance stage of the production lifecycle, but that does not specifically regulate technology.

2.6.1.4 Example 4: SBNs – Performance-Based Regulation That Specifies the Means of Achieving Performance

Security Breach Notification laws are designed to achieve two output conditions: 1) that individuals will know when their personal information has been compromised;[61] and 2) a

[57] 45 C.F.R. § 164.306(b)(2)(ii)(1).
[58] 45 C.F.R. § 164.306(d)(3).
[59] 45 C.F.R. 164.306(b)(1).
[60] In the author's experience in private practice, these regulations do afford organizations with wide latitude as to the implementation details involved in compliance with these aspects of administrative security requirements of HIPAA.
[61] *See* infra n. 109.

coincident reduction in the number of breaches involving unencrypted personal information as organizations become increasingly aware of the risk of compromise and as public and media attention is drawn to organizations that experience breaches.[62] As discussed in greater detail below,[63] SBNs accomplish these goals through a regulatory framework that requires organizations to disclose when they experience data breaches involving certain types of personal information. This approach suggests a focus on regulating performance, similar to C&L's performance-based regulation. C&L's model, however, does not consider regulation that regulates performance *and* (directly or indirectly) specifies *how* that performance must be achieved.[64]

Nearly all SBNs have a "safe harbor" exception for encrypted data, under which breaches involving personal information that was encrypted need not be disclosed.[65] The CISO interviews revealed that organizations attempted to address the "problem" of disclosing security breaches not by focusing greater resources on mitigating risk to *prevent* breaches, but rather by focusing resources to mitigate risk *after* a breach by encrypting personal information.[66] In theory, both approaches reduce the number of reportable incidents, although an interesting topic for further research would be to investigate which approach had a better "return-on-investment" as a function of cost per reduced breach. It is important to note that the encryption approach does not necessarily reduce the number of incidents that would otherwise qualify (but for their lack of including the "exact" combinations of personal information) as breaches under SBNs. Furthermore, it does not necessarily imply that the data actually was rendered useless to an attacker, as there is no

[62] Although not specifically part of the debates in the California Legislature, it seems perhaps obvious that the intent of a statute designed to publicly highlight an organization's security failures would also be to reduce the number of such failures. This conclusion is further strengthened when considering states such as Massachusetts and New York which have centralized reporting requirements to state regulators, in addition to consumer reporting requirements, in the event an organization experiences a qualifying breach.
[63] *See* Section 2.7.1.
[64] Coglianese and Lazer at 701 (". . . a performance standard specifies the level of performance require of a firm but does not specify how the firm is to achieve that level").
[65] *See* Section 2.7.1.
[66] This research directly revealed a focus on encrypting portable devices (e.g., laptops) that store personal information, and also indicated a focus on encrypting other resources that store personal information.

mathematically-sound statutory definition[67] of qualifying encryption in the SBNs (e.g., a "broken" encryption algorithm could qualify).[68]

In either event, however, my research suggests the predominant approach (encryption) results in a condition under which regulation is "targeted" to affect one stage in the production lifecycle yet indirectly produces regulatory results in another. Specifically, the aspects of SBNs examined here regulate based on efficacy of information security (e.g., a reporting "penalty" applies if security measures fail and a qualifying breach occurs). They do not specify how an organization *must* achieve the efficacy goal, however they do indirectly suggest an approach (encryption). As mentioned above, and discussed in detail in Section 2.7.1.3, the result is what C&L's framework would likely describe as a performance-based regulation. SBNs, however, primarily achieve an effect at the implementation/maintenance stage, which under C&L's framework is reserved for technology-based regulation. The primary target and primary effect of the regulation occur at different stages in the production lifecycle.

A faceted classification approach provides a solution to this problem. Allowing regulations to be categorized as affecting more than one stage of the production lifecycle provides the flexibility to address part of this problem. Further separation is necessary, however, to achieve the level of granularity ideal for a complete framework. Specifically, as identified in this example, the target and effect of a regulation may occur at different stages in the productive lifecycle. Furthermore, the effect of regulation may be the result of a regulatory aspect other than the intended primary goal. As a result, a complete framework must distinguish between the aspect of what a regulation targets and what practice effects a regulation achieves. It is important to note that examining this distinction necessarily implies the use of empirical methods of analysis in categorizing regulations.

[67] *See, e.g.,* Cal. Civ. Code § 1798.82(a) (lacking any definition of "encryption"); *see also, e.g.,* IOWA CODE § 715C.1(5) (defining encryption as "the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key," a definition that would likely *not* preclude the use of a an encryption algorithm against which there is a known attack (*see* n. infra 68)).

[68] Under the existing statutory language, a lost laptop containing two version 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* in note 67. This particular implementation of RC-4, however, while operating at a 128-bit encryption keylength, has a known vulnerability under which an attacker can break the encryption with minimal effort. *See* 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.

2.6.2 Distinguishing HIPAA and GLBA from Other Notice-and-Comment Rulemaking

Certain information security regulatory structures rely on a fundamental concept of "reasonable security." This concept, not unlike other forms of regulation, presumes that a one-size-fits-all approach to regulating is not optimal[69] 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 C&L's conception of management-based regulation, as discussed in Section 2.3.1.3. However, as discussed in Sections 2.5.3 and 2.6.1.3, their definition fails to adequately capture the character of these laws for the purposes of understanding information security regulation. Sections 2.7.2 and 2.7.3 discuss alternative means to understanding HIPAA and GLBA (respectively) consistent with the revised framework I propose in Section 2.6.3. This groundwork explains what HIPAA and GLBA are – regulatory frameworks that seek input from industry professionals in the establishment of the 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:[70] 1) legislation that is merely prescriptive, and does not provide rulemaking authority to administrative agencies; 2) legislation that delegates rulemaking authority to administrative agencies but does not specify deference to industry; and 3) legislation that delegates rulemaking authority to administrative agencies and specifies that those agencies should defer to industry standards in the rulemaking process. The first category describes regulation I discuss in Section Chapter 4, Section 4.1.2 below which 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.

[69] *See* Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L. J. 377, 387 (2006) (describing how "[o]ne-size-fits-all rules cannot easily account for the ways in which risk manifests itself differently across firms").

[70] Special thanks to my Dissertation Chair, Deirdre K. Mulligan, for her assistance in the development of this approach to distinguishing HIPAA and GLBA from other forms of notice-and-comment rulemaking.

2.6.2.1 Prescriptive Legislation

Prescriptive 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)[71] and the Electronic Communications Privacy Act (ECPA).[72] The VPPA specifies limitations on the disclosure of personally identifiable information[73] of consumers who rent, purchase, or subscribe to other goods and services from a video tape service provider.[74] The restriction is straightforward, and the statute does not prescribe any rulemaking authority nor even reference the involvement of an administrative agency in the regulatory process.

ECPA operates in a similar fashion. It makes unlawful interception[75] of wire communications a felony[76] and specifies precisely what constitutes unlawful interception and what exceptions exist.[77] Like the VPPA, ECPA neither prescribes rulemaking authority for any administrative agency – even the Federal Communications Commission – nor references the involvement of any such agency, except as to referencing previously-existing FCC rules for descriptive purposes.

SBNs, which I discuss extensively elsewhere[78] throughout this paper, 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. 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, and I discuss how regulation links to professionalism in Chapter 4, Section 4.1.2.

[71] Video Privacy Protection Act, Pub. L. No. 100-618 (codified as amended at 18 U.S.C. §§ 2710-11).
[72] Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-11).
[73] 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." 18 U.S.C. § 2710(a)(3).
[74] 18 U.S.C. § 2710(b)(1).
[75] 18 U.S.C. § 2511(1)(a).
[76] 18 U.S.C. § 2511(4)(a).
[77] 18 U.S.C. § 2511(2).
[78] *See, e.g.,* Sections 3.1, 3.9.4.3, 2.6.1.4, and 2.7.1.

2.6.2.2 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. The agency publishes notices to this effect in the Federal Register, inviting the public (and more specifically, interested parties) to submit comments. The agency then considers these comments and drafts regulations pursuant to the authority granted it by Congress. 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.[79]

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”)[80] and the Fair Credit Reporting Act (“FCRA”).[81] COPPA, for example, specifies that the Federal Trade Commission shall implement regulations to ensure various protections with respect to children’s usage of websites (see Appendix F.1 for complete excerpt).[82]

These regulations require the FTC to, subject to the requirements of the Administrative Procedures Act (“APA”),[83] promulgate regulations to achieve the intent specified above. The APA does not specifically require the FTC (or any other federal agency) to defer the judgment of private industry or professionals in the promulgation of those rules. FCRA has similar requirements.[84]

Delegating these responsibilities to the FTC (and other financial regulatory agencies) makes sense. Developing rules for consumer notification procedures are within the core competencies of the Commission. Likewise, developing rules governing the use of consumer reports and related financial information are within the core competencies of the Commission and the other financial regulatory agencies referenced in FCRA.

[79] *See* Richard B. Stewart, *The Reformation of American Administrative Law*, 88 HARV. L. REV. 1669, 1683-88 (providing a thorough discussion of the administrative agency rulemaking process, with specific relevant emphasis at the pages noted, and a critique of this process).

[80] Children’s Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2581 (codified as amended at 15 U.S.C. §§ 6501-6506).

[81] Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1114 (codified as amended at 15 U.S.C. §§ 1681-1681u).

[82] 15 U.S.C. § 6502(b).

[83] *See* Administrative Procedures Act, Pub. L. 79-404, 60 Stat. 237 (codified as amended at 5 U.S.C. § 500 *et seq.*).

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

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 compared to other traditional notice-and-comment rulemaking. The difference lies in Congress' command to the regulatory agencies with respect to the rulemaking process and the differences in the core competencies of the relevant agencies[85] at the time HIPAA and GLBA were passed.

2.6.2.3 Notice-and-Comment Rulemaking with Deference to Industry ("Regulatory Delegation")

As discussed above, 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. 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).

In the case of the HIPAA Privacy Rule, for example, Congress specifically required that:[86]

> (d) 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.

The National Committee on Vital and Health Statistics comprises key stakeholders in the health and health information policy fields from industry, government, and academia.[87] 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

[85] 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* supra n. 142).

[86] 42 U.S.C. § 1320d-2(d).

[87] *See* Introduction to the NCVHS, http://www.ncvhs.hhs.gov/intro.htm (last visited Apr. 8, 2011), *see also* 42 U.S.C. § 242k(k)(2).

research, consumer interests in health information, health data standards, epidemiology, and the provision of health services."[88] The Committee also is responsible for assisting the Secretary in promulgating rules relating to the HIPAA "Security Rule"[89] which governs the information security requirements for the interchange of health-related information.[90]

In the case of GLBA, Congress' command is not as clear. The Act requires that:[91]

> (b) . . . each [of the 8 GLBA regulators] 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.

It specifies that, with respect to rulemaking in this regard:[92]

> (1) The Federal banking agencies, the National Credit Union Administration, the Secretary of the Treasury, the Securities and 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 subtitle with respect to the financial institutions subject to their jurisdiction under section 505; and

[88] *Id*. The full committee membership is available online at http://www.ncvhs.hhs.gov/members.htm.

[89] *See* 42 U.S.C. § 1320d-2(d).

[90] *See* 42 U.S.C. § 242k(k)(5)(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), 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);" 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 "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").

[91] 15 U.S.C. § 6801.

[92] 15 U.S.C. § 6804.

> (2) 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.

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. 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[93] and supported by my quantitative analysis.[94] 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 HIPAA than that conducted with ordinary notice-and-comment procedures under the APA.

2.6.3 "Tagging" Using a Faceted Classification System

The examples in Section 2.6.1 above describe failures of C&L's strict typology to accurate and precisely describe information security laws. Section 2.6.2 above describes how the process for participation by private stakeholders in the rulemaking process varies, a parameter not considered in C&L's typology. To address these shortcomings, I propose describing information security laws using a faceted classification system.

Faceted classification systems are means for describing the category into which an item falls by a series of facets, or subparts of a larger category, together which comprise a complete description of the category. Unlike classical categorization theory,[95] in which categories are defined by properties all of which all members of the category share, faceted classification systems allow for categorization based on the intersection of each of the attributes describing a phenomenon. As described by Taylor:

> If one thinks of each of the faces of a cut and polished diamond as a facet of the whole diamond, one can picture a classification notation that has small notations

[93] *See* Chapter 1, Section 3.9.3.
[94] *See* Chapter 1, Section 3.7.5.
[95] Arlene G. Taylor, THE ORGANIZATION OF INFORMATION 300 (2d ed. 2004).

> standing for the subparts of the whole topic strung together to create a complete classification notation.[96]

Here, instead of faces of a diamond, the parameters characterizing a regulation are "strung together" to create a complete classification of that regulation. This section discusses how I apply such an approach to create a complete framework capable of addressing the shortcomings identified about Coglianese and Lazer's model in the sections above.

One approach to addressing the issue of mixed-target regulations, where a regulation targets more than one stage in the production lifecycle, is to "break apart" or consider separately the multiple aspects of the regulation. For example, a regulation such as that discussed in Section 2.6.1.2 above requiring the use of technological countermeasures, could be viewed both as targeting the implementation/maintenance stage and as targeting the efficacy/output stage. Under this approach, the two aspects of the regulation could be analyzed separately, thus facilitating use of a strictly-typed singular framework like Coglianese and Lazer's. In Section 2.6.1.4 above, however, I introduce the concept of regulations that target one stage of the production lifecycle but have regulatory impact, or effect, at another stage. Regulations falling into this category are a fundamental reason why breaking apart mixed-target regulations into their constituent elements for analysis will not provide a complete framework to categorize information security laws and regulations.

Considering all of the factors described throughout this section, traditional singular frameworks do not provide a solution appropriate to categorizing information security laws and regulations. Instead, therefore, I propose a system under which regulation is classified according to four parameters, each of which represents one facet. Under this system, regulations can then be "tagged" with various classifications, each comprising a set of values (one for each of the four parameters) and multiple tags may be applied to describe a given law or regulation.

2.6.3.1 Parameter 1: Functional Character of the Regulation

The first parameter is the character of the regulation, and describes "how" the regulation functions. This parameter borrows from Coglianese and Lazer's framework, describing a

[96] *Id*. at 302.

regulation as one of management-based, means-based,[97] or production-based. These definitions mirror the functional elements of their framework, but ignore the chronological ties to the production lifecycle and constraints related to the use of the term "technology."[98]

The descriptor "management-based regulation" applies when a regulation's purpose is to require some type of planning, risk-assessment, or other internal process, the results of which should produce a course of action (or information thereabout) for the organization to follow. Although most commonly targeted at the design/planning stage of the production lifecycle,[99] such regulations may require these activities at other stages. A regulation that requires organizations to implement policies and procedures to address security incidents,[100] for example, would target the efficacy/output stage. Such a regulation might also affect the implementation/maintenance stage (e.g., because certain logging/auditing activities may be necessary to facilitate post-incident investigation) and/or have secondary targets at this stage (e.g., by requiring that corrective steps, such as virus/malware scanning, be taken immediately following an incident rather than during their normally-scheduled times). The key element of management-based regulation is the "requirement to analyze" and (possibly) act on that analysis.

The descriptor "means-based regulation" applies when a regulation's purpose is to define specific technologies, methods, or processes that must be followed at a given stage in the production lifecycle. Means-based regulation is traditionally associated with the implementation/maintenance stage of the production lifecycle.[101] In the context of information security, however, it is commonly associated with each of the three stages of the production lifecycle. Its distribution across all stages may be a result of information security's uncommon characteristic of being both a "good" and a "process" as discussed above at the beginning of Section 2.4.

The descriptor "performance-based regulation" applies when a regulation's purpose is to define specific goals or output conditions that an organization must obtain. Regulation may do so explicitly, by directly expressing a requirement, or implicitly, by assigning

[97] I propose a friendly renaming of "technology-based" to "means-based." In the information security space, the word "technology" carries with it specific connotations (e.g., there are administrative, physical, and *technical* measures involved in any comprehensive information security program). Describing this aspect of the functional character of the regulation as "means-based" makes the definition more descriptive and perhaps more palatable to technical readers of this work.
[98] *See* supra n. 97.
[99] Coglianese and Lazer at 693-94.
[100] *See, e.g.,*, 45 C.F.R. § 164.308(a)(6) (requiring that organizations "[i]mplement policies and procedures to address security incidents," specifically that HIPAA covered entities "[i]dentify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.").
[101] Coglianese and Lazer at 693-94.

consequences for failures to do so (e.g., the consumer notification requirement of SBNs). Performance-based regulation is most commonly associated with the output/efficacy stage of the production lifecycle.[102] The nature of information security as both a "good" and a "process," however, does create the possibility of performance-based regulation that targets another stage in the production process as discussed above in Section 2.6.1.2. Furthermore, as discussed above in Section 2.6.1.4, a performance-based regulation that targets the output/efficacy stage may have an effect on another stage (e.g., as in the SBN example described above).

2.6.3.2 Parameter 2: Intent of the Regulation

The second parameter describes whether the aspect of the regulation being analyzed is one that specifically "targets" the behaviors its text describes or one that produces a secondary or unintended behavioral "effect." The genesis for incorporating this distinction was the predominant theme throughout the CISO interviews that SBNs produce an unintended compliance-like effect, discussed in greater detail in Section 2.7.1.3, of incentivizing organizations to encrypt the data storage on all their portable devices. This distinction allows regulations such as SBNs to be characterized, or "tagged," both by their (apparent) textual intent, and by their (observed) empirical effect. A tag containing the "target" parameter will almost always be the result of textual analysis of the statute or regulation in question, whereas a tag containing the "effect" parameter will almost always be the result of analysis of empirical data. This analysis may be quantitative in nature[103] or make use of qualitative data such as the CISO interviews.[104]

2.6.3.3 Parameter 3: Chronological Impact of the Regulation

The third parameter is the point in the production lifecycle that regulation impacts. It describes that production stage at which regulation either targets or affects the behavior of the regulated entity. As discussed at length throughout this section, the stage impacted by regulation may differ from that traditionally associated[105] with the functional character of the regulation. Thus this parameter is included to address these cases where the functional character and the impacted product stage do not match traditional associations.

[102] *Id.*

[103] *See, e.g.*, Chapter 1, Section 3.7.

[104] The inclusion of the "effect" parameter does introduce a requirement for empirical analysis into this framework, however it seems implausible to characterize the "real-world" effects of any regulatory regime without some empirical observation and thus I do not view this requirement as unduly burdensome for researchers seeking to employ or improve upon my proposed framework.

[105] *See* Coglianese and Lazer at 693-94.

For the purposes of this parameter, I borrow from Coglianese and Lazer's construction of the production lifecycle for goods and services.[106] As discussed above in this Section and in Section 2.3.1, they conceive of three stages in the production lifecycle: 1) Planning; 2) Acting; and 3) Outputs (both good and bad). Earlier in this section I propose revising these terms to ones more descriptive of the nuances in information security, with particular consideration for the character of information security as both a "good" and a "process." Accordingly, the three choices for this parameter are: 1) the Design/Planning Stage; 2) the Implementation/Maintenance Stage; and 3) the Output/Efficacy Stage. Section 2.6.1.1, 2.6.1.2, and 2.6.1.4 above provide examples of what types of regulation fall into each stage.

2.6.3.4 Parameter 4: Involvement of Private Parties in the Rulemaking Process

The fourth parameter describes to what extent, if any, private parties may participate in the rulemaking process for information security regulation. As described in Section 2.6.2 above, there are three types of regulatory approaches to private party involvement: 1) prescriptive legislation; 2) traditional notice-and-comment rulemaking; and 3) notice-and-comment rulemaking with deference to industry.

Under prescriptive legislation, the legislature fully defines the parameters and rules in a given piece of legislation. While administrative agencies may be charged with enforcement, those agencies are not provided instruction (or discretion) to implement rules pursuant to the legislation. The legislation's instructive effect is limited to the text of the actual bill enacted into law.[107]

Under traditional notice-and-comment rulemaking, the legislature enacts a law which also directs an administrative agency to conduct a rulemaking process filling in certain "details" of the law. As described above, under the Administrative Procedures Act, this rulemaking process includes an opportunity for private parties to submit comments to the administrative agency. However, no special deference must be given to these comments and the agency is free to disregard them.

Notice-and-comment rulemaking with deference to industry, or "regulatory delegation," differs from traditional notice-and-comment rulemaking. In regulatory delegation models, the legislature expressly *instructs* the administrative agency to consult with and

[106] *Id*. at 693-94.

[107] And, obviously, any judicial interpretation of that law. Since judicial interpretation is possible in all three cases of this parameter, its effect does not vary across values for the parameter and therefore is not instructive for this analysis.

give deference to the input of private party stakeholders, particularly the relevant private industrial entities who will be subject to the promulgated regulations.

Unlike the other parameters in my proposed typology, this parameter generally applies uniformly across each law under consideration. Multiple classifications are not generally applicable to a single law, and therefore for the purposes of my analysis each law or regulation matches exactly one of the categories above.

2.7 CLASSIFYING INFORMATION SECURITY REGULATIONS

This section applies the typology I propose above to characterize each of the primary information security regulatory frameworks. I draw upon the CISO interviews as empirical data to reinforce my analysis of the statutory, regulatory, and adjudicative text. The sections that follow discuss each law generally, classify it according to the degree to which it involves private parties (parameter 4), and identify what other combinations of parameters 1 through 3 apply to each law.

2.7.1 Security Breach Notification Laws (SBNs)

Security Breach Notification statutes are laws requiring an organization that loses control of "personal information" it maintains about individuals to disclose that loss to those individuals. As of October 2010, 46 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have such laws.[108] 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.[109]

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. The two sections that follow examine the two component elements of Hypothesis **H1**.

[108] *See* State Security Breach Notification Laws, http://www.ncsl.org/Default.aspx?TabId=13489 (last visited Feb. 14, 2011).

[109] *See, e.g.*, CAL. BILL ANALYSIS, S.B. 1386, Cal. Assembly, 2001-2002 Reg. Sess. (Aug. 23, 2002) (Senate Third Reading, analysis of Saskia Kim) ("CA SBN Debates").

2.7.1.1 SBNs Are Prescriptive Legislation

To date, no state's SBN statute involves either a rulemaking process by an administrative agency.[110] Rather, the text of the statute fully specifies all aspects of the notification requirements and exemptions.[111] In this regard, SBNs are clearly prescriptive legislation.

2.7.1.2 SBNs Are Performance-Based Regulation Targeting the Output/Efficacy Stage

On their face, SBNs appear to be traditional performance-based regulation 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[112] – 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[113] 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

[110] The Massachusetts Data Security Standards, discussed in greater detail in Section 2.7.5 below, 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. *See* MASS. GEN. LAWS ch. 93H, § 2.

[111] Massachusetts statute does define the meaning of "encrypted" in its statutory text. *See* MASS. GEN. LAWS ch. 93H § 1(a). It is worth noting that Massachusetts' 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." *See* MASS. GEN. LAWS ch. 93H §1(b). However, it neither *requires* the Department to do so nor does it yet appear that were the Department to do so that it would have anything more than a marginal impact on the applicability of the statute.

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

[113] *See* N.Y. GEN. BUS. LAW § 899-aa(1)(b) (defining "'private information' [to 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."); *see also* § 899-aa(1)(a) (defining "'personal information' [to 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.").

> 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 breach and restore the reasonable integrity of the system.[114]

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.

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.[115] 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. Since 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.[116] 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."[117] Specifically, the legislature sought to accomplish this by establishing law requiring organizations to make consumers aware of when their data was compromised.[118] 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. It is, however, important to note and raises the question of whether the law is actually effective at achieving this goal.

[114] N.Y. Gen. Bus. Law § 899-aa(2).

[115] New York State also has a centralized notification requirement (N.Y. GEN. BUS. LAW § 899aa(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 (N.Y. GEN. BUS. LAW § 899aa(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.

[116] *See, e.g.,* CONN. GEN. STAT. § 36(a)-701; *see also, e.g.,* CAL. CIV. CODE §§ 1798.81.5 – 1798.82; *see also* State Security Breach Notification Laws, http://www.ncsl.org/Default.aspx?TabId=13489 (last visited Feb. 14, 2011) (providing a current listing of and citations to all U.S. jurisdictions with SBNs).

[117] CA SBN Debates at 2.

[118] *Id.*

That question is explored in part in Section 2.7.1.3 below (inasmuch as it was addressed by the respondents) and again later in Chapter 4, Section 4.1.2.

2.7.1.3 SBNs are Means-Based Regulation Affecting the Implementation/Maintenance and Design/Planning Stages

Interviews with CISOs revealed the surprising result that SBNs had a predominant effect of driving the implementation of technical practices. Specifically, organizations began to institute unilateral laptop/portable media encryption policies. This was done not in response to any particular evidence that doing so would decrease the number of individuals whose identity was stolen as a result of data breaches,[119] 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 my 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.

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. These policies clearly 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." 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,[120] the language in this instance makes clear that effect occurs at the implementation/maintenance stage in this respondent's organization.[121] Finally, although

[119] This is not to say that doing so would not have an effect in reduce identity theft, nor is it to say that encrypting portable media is an ineffective security practice.

[120] E.g., a policy that an organization's security professionals must design a system scanning all future (and possibly existing) data for qualifying "sensitive information" and, when such information was found, it would 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 suggested by the language of this respondent.

[121] 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).

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. As discussed above in Section 2.7.1.1, 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.

Another respondent identified this same effect of SBNs driving encryption, although interestingly did so in a more positive context. 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":

> . . . 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].

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. The respondent further notes that they find this style of approach preferably "[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.

While both respondents identify a condition supporting the proposition that SBNs have an effect of driving the use of encryption technology, thus supporting the hypothesis of this section, 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 Chapter 4, Section 4.1.3.

2.7.2 Health Insurance Portability and Accountability Act Security and Privacy Rules ("HIPAA")

The Health Insurance Portability and Accountability Act[122] was passed in 1996 as part of broad effort to reform various aspects of the healthcare and health insurance systems in the United States. 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. This information is collectively termed Protected Health Information ("PHI")[123] and includes:[124]

> (6) . . . any information, including demographic information collected from an individual, that--
>
> > (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
> > (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and--
> >
> > > (i) identifies the individual; or
> > > (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

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. Covered Entities are defined as:[125]

> (1) A health plan.
> (2) A health care clearinghouse.
> (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

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 (see Appendix F.2). [126]

[122] Health Insurance Portability and Accountability Act of 1996, Pub. L. 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.).

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

[124] 42 U.S.C. § 1320d.

[125] 45 C.F.R. § 160.103.

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 apply to all healthcare insurance organizations, processing organizations that support healthcare insurance organizations, medical providers (if they use electronic records), and any other entities who engage in business with them if that transaction of business involves the exchange or handling of PHI.

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;[127] and 2) a general instruction to organizations covered by the Rule that they maintain appropriate administrative, technical, and physical safeguards.[128] The first element is the key provision under which specific information security regulations part of HIPAA are promulgated:[129]

> (1) SECURITY STANDARDS.--The Secretary shall adopt security standards that--
>
> (A) take into account--
>
> (i) the technical capabilities of record systems used to maintain health information;
>
> (ii) the costs of security measures;
>
> (iii) the need for training persons who have access to health information;
>
> (iv) the value of audit trails in computerized record systems; and
>
> (v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and
>
> (B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.

The regulations promulgated by the Secretary of Health and Human Services pursuant to this provision[130] are too numerous to list here in a comprehensive fashion, nor would

[126] *Id*.

[127] 42 U.S.C. § 1320d-2(d)(1).

[128] 42 U.S.C. § 1320d-2(d)(2).

[129] 42 U.S.C. § 1320d-2(d).

[130] *See* Administrative Data Standards and Related Requirements – Security and Privacy – General Provisions, 45 C.F.R. §§ 164.102 – 164.534.

doing so 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. This examination, which follows, is informative as to classifying HIPAA's Security Rule according to the framework I propose in Section 2.6.

As suggested by Hypothesis **H2**, 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. The HIPAA regulations also specify certain protection measures that regulated organizations must undertake, similar to means-based regulation. Unlike traditional means-based regulation, however, the regulations do not specify the implementation details for those measures, but rather explicitly leave those to the regulated entities. In the next two sections, I explore each of these respectively and propose that HIPAA is therefore a form of management-based regulation that affects each of the Design/Planning and the Implementation/Maintenance stages of the ISPL.

2.7.2.1 HIPAA is a Form of Regulatory Delegation

As discussed above in Section 2.6.2.3 in greater detail, HIPAA involves a notice-and-comment process with legislative direction to give deference to key stakeholders. It specifically requires[131] 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.

2.7.2.2 HIPAA is Management-Based Regulation Targeted at the Design/Planning Stage of the ISPL

The regulations promulgated under the HIPAA Security Rule bear many of the aspects of traditional management-based regulation under C&L's typology. The general requirements[132] and flexibility of approach[133] specified in the general rules for security standards require organizations to:[134]

> (a) General requirements. Covered entities must do the following:

[131] *See* 42 U.S.C. § 1320d-2(d)(1).
[132] 45 C.F.R. § 164.306(a).
[133] 45 C.F.R. § 164.306(b).
[134] 45 C.F.R. § 164.306(a).

> (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
> (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
> (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
> (4) Ensure compliance with this subpart by its workforce.

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:[135]

> (b) Flexibility of approach.
>
> (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
> (2) In deciding which security measures to use, a covered entity must take into account the following factors:
>
> (i) The size, complexity, and capabilities of the covered entity.
> (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
> (iii) The costs of security measures.
> (iv) The probability and criticality of potential risks to electronic protected health information.

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"[136] and to "[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)."[137] These directives to conduct risk assessments and implement security measures consistent with those risk assessments are a perfect example of traditional management-based regulation.

[135] 45 C.F.R. § 164.306(b).
[136] 45 C.F.R. § 164.308(a)(1)(ii)(A).
[137] 45 C.F.R. § 164.308(a)(1)(ii)(B).

2.7.2.3 HIPAA is Management-Based Regulation Targeted at the Implementation/Maintenance Stage of the ISPL

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 – taking it almost to the degree of means-based regulation, but stopping short in leaving the details of implementation at the discretion of the regulated entity consistent with the flexibility of approach provisions outlined above.[138] Consider the following four provisions of the HIPAA Security Rule regulations:[139]

> (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 information.

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)." 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. 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. As discussed later in Section 4.1.1.2.2, this bifurcation has implications for the relationship between senior managers and information security professionals at regulated organizations.

[138] *See* 45 C.F.R. § 164.306(b); *see also* Section 2.7.2.1.
[139] 45 C.F.R. § 164.312(a)(2).

2.7.3 Gramm-Leach-Bliley Financial Modernization Act ("GLBA")

The Gramm-Leach-Bliley Financial Modernization Act of 1999[140] ("GLBA") specifies requirements for Financial Institutions Safeguards Rule[141] ("Safeguards"). The Safeguards require that:

> each agency or authority described in [15 U.S.C. § 6805(a)] shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards--
>
> > (1) to insure 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.

The Safeguards require each of the agencies[142] charged with enforcing the provisions of GLBA to promulgate regulations implementing the Rule. The FTC has promulgated a series of regulations pursuant to the Safeguards, which they call the "Safeguards Rule."[143] 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"[144] ("Interagency Guidelines"). I examine

[140] Gramm-Leach-Bliley Financial Modernization Act of 1999, Pub. L. 106-102, 113 Stat. 1338 (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.).

[141] 15 U.S.C. § 6801(b).

[142] At the time of its enactment, GLBA charged seven federal regulatory agencies with enforcing the privacy and security provisions of 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)(1)-(7). § 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 § 6805(a). This is particularly interesting considering the CFTC recent promulgated regulations pursuant to the GLBA Privacy rule. *See* Elizabeth A. Khalil, *CFTC Proposes Rules on Affiliate Marketing, Data Disposal, and GLBA Privacy*, http://www.hldataprotection.com/2010/10/articles/financial-privacy/cftc-proposes-rules-on-affiliate-marketing-data-disposal-and-glba-privacy/ (last visited Oct. 28, 2010).

[143] *See* 16 C.F.R. § 314.

[144] *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005) (codified at scattered sections of 12 C.F.R.).

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 for which I interviewed CISOs, and based on those interviews, my experience in private practice, and discussions with practitioners, appear to be the predominant rules driving compliance. The two sections discussing the GLBA Safeguards Rule collectively examine the elements of Hypothesis **H3a**, and the two sections discussing the Interagency Guidelines collectively examine the elements of Hypothesis **H3b**.

2.7.3.1 GLBA is a Form of Regulatory Delegation

As discussed above in Section 2.6.2.3 in greater detail, GLBA has some aspects that suggest Congress intended to involve industry in the notice-and-comment rulemaking process. Additionally, as discussed above, the CISO interviews revealed that financial institutions had substantial incentive to participate in this process. While not as stark an example as HIPAA, it appears that Congress' intent with respect to GLBA was more oriented toward a regulatory delegation model than toward the traditional notice-and-comment process.

2.7.3.2 The FTC's GLBA Safeguards Rule is a form of Management-Based Regulation Targeting the Design/Planning Stage of the ISPL

The FTC regulations are particularly notable because, as discussed in further detail in Section 2.7.4, the Safeguards Rule guided certain key elements of the FTC's jurisprudence in their privacy and data security enforcement actions. The implementing regulations promulgated by the FTC specify:

> (a) Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.
>
> (b) Objectives. The objectives of section 501(b) of the Act, and of this part, are to:
>
> > (1) Insure the security and confidentiality of customer information;
> >
> > (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
> >
> > (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

These regulations are a classic example of management-based regulation. They require individual regulated organizations to development 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 it wide discretion to innovate in selecting approaches for compliance. This is precisely consistent with the concept of management-based regulation discussed above in Sections 2.3.1.3 and 2.6.3.1.

2.7.3.3 The FTC's GLBA Safeguards Rule is a form of Management-Based Regulation Targeting the Output/Efficacy Stage of the ISPL

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 "in order to develop, implement, and maintain [a] information security program, [regulated organizations] shall" engage in a specified series of activities to design and maintain that plan. 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 provides to ensure their activities are consistent with the plan, and periodic evaluation and revision of the information security plan.[145] The full text of the regulation is provided in Appendix F.3.

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 requiring regulated organizations to "regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems and procedures"[146] and "evaluat[ing] and adjust[ing] [the] information security program in light of the results of [that testing]."[147] 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 suggest that the Output/Efficacy Stage is substantially targeted by this regulation.

[145] 16 C.F.R. § 314.4.
[146] 16 C.F.R. § 314.4(c).
[147] 16 C.F.R. § 314.4(e).

2.7.3.4 The GLBA Interagency Guidelines on Information Security are a form of Management-Based Regulation Targeting the Design/Planning Stage of the ISPL

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 an information security plan:[148]

> A. Information Security Program. Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.
>
> B. Objectives. A bank's information security program shall be designed to:
>
> > 1. Ensure the security and confidentiality of customer information;
> > 2. Protect against any anticipated threats or hazards to the security or integrity of such information;
> > 3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
> > 4. Ensure the proper disposal of customer information and consumer information.

Just as with the FTC's GLBA Safeguards Rule above, these regulations represent classic example of management-based regulation. They require individual regulated organizations to development 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 it wide discretion to innovate in selecting approaches for compliance. This is precisely consistent with the concept of management-based regulation discussed above in Sections 2.3.1.3 and 2.6.3.1.

[148] 12 C.F.R. § 30, App. B § (II).

2.7.3.5 The GLBA Interagency Guidelines on Information Security are a form of Management-Based Regulation Targeting the Implementation/Maintenance Stage of the ISPL

Like the HIPAA regulations discussed above in Section 2.7.2.3, the Interagency Guidelines also specify in detail what elements an information security program must contain and what goals those elements much achieve. The full text of these requirements is provided in Appendix F.3. 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.[149]

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.

2.7.4 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 and/or sensitive information. Their primary statutory basis[150] for doing so was Section 5 of the FTC Act, which grants the Commission the authority to investigate and challenge business practices it finds unfair or deceptive.[151] Pursuant to this authority, the FTC brought several enforcement

[149] 12 C.F.R. § 30, App. B § (III)(C).

[150] There are a number of other secondary statutory basis upon which the FTC rests their data security enforcement actions, including the Fair Credit Reporting Act (15 U.S.C. §§ 1681-1681u), the Fair and Accurate Credit Transactions Act of 2003 (FACTA) (15 U.S.C. §§ 1681-1681x), the Health Information Technology for Economic and Clinical Health Act (Pub. L. 111-5, 123 Stat. 226 (codified in scattered parts of 42 U.S.C.)), the Gramm-Leach-Bliley Financial Modernization Act (discussed above in Section 2.7.3, *see also* supra n. 140), and the Children's Online Privacy Protection Act (15 U.S.C. §§ 6501-6505). For the purposes of this section, with the exception of GLBA, these secondary basis are unimportant as to the classification of the FTC's jurisprudence according to my revised typology of information security regulation.

[151] *See* 15 U.S.C. § 45(a)(1).

actions[152] against organizations it believed to have engaged in "unfair or deceptive" information security practices violative of Section 5. Generally speaking, the Commission asserted as "deceptive" those practices where organizations promised one level of security and failed to deliver that level of security,[153] 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.[154]

In practice, nearly all these matters result in a settlement between the organization under investigation and the Commission. These settlements generally include the following elements: 1) an agreement to discontinue and/or correct the offending information security practices; and 2) an agreement to engage in ongoing periodic information security assessments the results of which must be attested to by a certified professional.[155] In rare circumstances where the violation alleged is so severe and the resultant consumer harm alleged so grievous, the Commission may also require compensatory or punitive damages.[156] These consent decrees and settlements form the basis for the aspects of FTC data security enforcement that I use 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.

[152] 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 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. filed Feb. 10, 2006) *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf (regarding the complaint); *see also, e.g.*, 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. filed Jan. 30, 2006) *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf (regarding the form of settlement).

[153] *See, e.g.*, Complaint, *In the Matter of Microsoft Corp.*, FTC File No. 012-3240 at ¶¶ 19-20 (Dec. 20, 2002) *available at* http://www.ftc.gov/os/caselist/0123240/microsoftcmp.pdf; *see also, e.g.*, Complaint, *In the Matter of Twitter, Inc.*, FTC File No. 092-3093 at ¶¶ 13-17 (Jun. 24, 2010) *available at* http://www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf.

[154] *See, e.g.*, Complaint, *In the Matter of BJ's Wholesale Club, Inc.*, FTC File No. 042-3160 at ¶¶ 9-10 (Sept. 20, 2005) *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf; *see also, e.g.*, Complaint, *In the Matter of The TJX Cos., Inc.*, FTC File No. 072-3055 at ¶¶ 11-13 (Mar. 27, 2008) *available at* http://www.ftc.gov/os/caselist/0723055/080327complaint.pdf.

[155] *See* Chapter 1, Section 3.4 above for a discussion of the professional(s) eligible to certify these assessments, and Section 4.1.1.2.2 below for a discussion of the implications of this attestation requirement for the role of information security professionals in organizations.

[156] Such matters often end up in federal District Court, *see* supra n. 152.

2.7.4.1 FTC Enforcement Action/Jurisprudence and Parameter 4

Parameter 4 of my faceted classification system describes statutes. The FTC's "jurisprudence" through its enforcement actions, as described above, is *pursuant* to statutory authority[157] but is not in itself a statute. For this reason, parameter 4 is inapplicable and not discussed in this context.

2.7.4.2 FTC Enforcement Actions are Management-Based Regulation that Target both the Design/Planning Stage and the Output/Efficacy Stage of the ISPL

As discussed above in Section 2.7.3, the initial and ongoing risk assessment requirement of the FTC's GLBA Safeguards Rule are 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:[158]

> 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.[citation omitted] 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.[citation omitted]

Like the risk assessment requirements in HIPAA and GLBA, the risk assessment requirements under the FTC's enforcement action settlements require organizations both to engage in an initial risk assessment within a specified period of time, develop an information security plan consistent with that risk assessment, and conduct periodic assessments thereafter and update their information security plans accordingly. Consider, for example, the excerpts from the Commission's settlement in the *BJ's Wholesale Club* matter[159] listed in Appendix F.5.

[157] *See* supra n. 150 and n. 151.

[158] Enhancing Data Security: The Regulators' Perspective: Hearing before the U.S. House of Representatives Subcomm. on Fin. Inst. and Consumer Credit of the Comm. on Financial Services, 109th Cong. (2005) (prepared statement of the Federal Trade Commission delivered by Lydia Parnes, Director of the Bureau of Consumer Protection of the Federal Trade Commission).

[159] *See* Decision and Order, *In the Matter of BJ's Wholesale Club, Inc.*, FTC File No. 042-3160 (Sept. 20, 2005) *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.

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, I do not see this difference as changing 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 as 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.

As noted above and described in the excerpted text, 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. As described above in Section 2.7.3.3, 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 ties the conduct of the periodic assessments to the outcomes sufficiently 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 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. This finding is consistent with Hypothesis **H4a**.

2.7.4.3 FTC Enforcement Actions are Means-Based Regulation that Target the Design/Planning and Implementation/Maintenance Stages

As noted above, the FTC enforcement actions and settlements contain provisions identifying the offending practices as "unfair" or "deceptive" and requiring the subject of the enforcement action to discontinue the offending practices. 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. 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.

The FTC alleged that verified incidents of identity theft resulted from these failures.[160] The Commission's specific allegations are listed in Appendix F.6.

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.[161] By effectively requiring the 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. This finding is consistent with Hypothesis **H4b**.

2.7.4.4 FTC Enforcement Actions are Means-Based Regulation Affecting all of the Design/Planning, Implementation/Maintenance, and Output/Efficacy Stages

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.

I describe this as a curious effect because, notwithstanding the analysis in Section 2.7.4.3 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

[160] *See* Complaint, *In the Matter of Reed Elsevier, Inc. and Seisint, Inc.*, FTC File No. 052-3904 at ¶ 12 (Mar. 27, 2008) *available at* http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf.

[161] *See* Agreement Containing Consent Order, *In the Matter of Reed Elsevier, Inc. and Seisint, Inc.*, FTC File No. 052-3094 at ¶ (II)(D) (Mar. 27, 2008) *available at* http://www.ftc.gov/os/caselist/0523094/080327agreement.pdf (explaining that the independent professional verifying the required security assessment must "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." Such a requirement would, obviously, include any facts alleged by the Commission to constitute "unfair" trade practices in violation of Section 5 of the FTC Act.).

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. From the legal scholar's perspective, this distinction may have import in evaluating the following classification I propose for such regulation.

I propose that, because of the practical effect of this regulatory process described above, the FTC's jurisprudence in identifying information security practices violative of Section 5 of the FTC Act constitutes a form of means-based regulation *affecting* each of the stages of the ISPL. I propose the characterization of means-based regulation for the same reason described in Section 2.7.4.3 above – the allegedly violative practices are specific, and therefore the avoidance thereof generally is also specific.[162] I propose the characterization of "affecting," rather than "targeting," because the enforcement actions from which these "requirements" arise have specific targets – they are not promulgated regulations. Finally, I suggest that these requirements affect all stages of the ISPL because, over the course of the FTC's information security enforcement, it has identified as allegedly unfair activities that address all three stages of the ISPL. Consider the following three examples: 1) a requirement to design strong authentication practices;[163] 2) a requirement to implement anti-virus software and intrusion-detection software, and to maintain ongoing efforts to detect network intrusions;[164] and 3) a requirement not to

[162] In certain cases it may leave some discretion in selecting alternate approaches to the individual organizations, however with many of the common examples – such as "failure to encrypt" or "failure to employ anti-virus software" – the obvious inverses of "encryption is required" and "anti-virus software is required" leave little limited discretion to the organization.

[163] *See* Complaint, *In the Matter of Reed Elsevier, Inc. and Seisint, Inc.*, FTC File No. 052-3904 at ¶ 10 (Mar. 27, 2008) *available at* http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf.

[164] *See* Complaint, *In the Matter of The TJX Cos., Inc.*, FTC File No. 072-3055 at ¶¶ 8(e) (Mar. 27, 2008) *available at* http://www.ftc.gov/os/caselist/0723055/080327complaint.pdf.

allow users' privacy as to their medication usage to be violated as a result of poor information security practices.[165]

It is difficult to empirically defend the characterization I propose above. Perhaps the greatest challenge is the inability of attorneys to reveal the advice they give their clients – I cannot, for example, report in this paper whether or not I advised a client to engage in a certain practice because of an FTC consent decree. I can state that generally, I would do so (as I have indicated above in this Section), however such reporting lacks the empirical rigor scholarship would ordinarily desire. Likewise, I suspect that a survey asking attorneys to publicly report how they would advise hypothetical clients would meet with substantial reticence. Notwithstanding these challenges, however, the CISO interviews did provide some insight suggestive that this characterization is valid. Consider, for example, the reply of one CISO of a large information technology company who described the *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.'"

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.

[165] *See* Complaint, *In the Matter of Eli Lilly & Co.*, FTC File No. 012-3214 at ¶ 7, 9 (Jan. 18, 2002) *available at* http://www.ftc.gov/os/2002/01/lillycmp.pdf (describing how "The June 27th disclosure of personal information resulted from respondent's failure to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information. For example, respondent failed to provide appropriate training for its employees regarding consumer privacy and information security; failed to provide appropriate oversight and assistance for the employee who sent out the email, who had no prior experience in creating, testing, or implementing the computer program used; and failed to implement appropriate checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the email" and how, therefore, "respondent has not employed measures and has not taken steps appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers through its Prozac.com and Lilly.com Web sites"). While the matter in question resulted in a privacy violation, it was this outcome – a privacy failure – upon which the complaint focused. The security examples given were only examples of procedures that, had they been in place, *might* have avoided the outcome. Therefore this focus on outcome – instead of design or procedure – suggests this as an outcome-based evaluation and, therefore, one appropriately described as (in the case of the respondent) targeting the output/efficacy stage of the ISPL.

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, as noted above, it does suggest support for Hypothesis **H4c**.

2.7.5 Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth ("Mass. Data Security Standards")

In early 2010, the Massachusetts Department of Consumer Affairs and Business Regulation promulgated regulations implementing the requirements of Massachusetts' law requiring "Regulations to Safeguard Personal Information of Commonwealth Residents."[166] The regulations were promulgated approximately 1-2 years after the CISO interviews were conducted and, as such, were neither considered in the design of those interviews nor discussed by any of the respondents. Nonetheless, I reference these regulations in several places in this paper and my experience in private practice suggests that at least some large organizations are concerned with the regulations. I therefore briefly discuss and suggest classifications for the regulations, with the caveat that these suggestions lack empirical basis in the CISO interviews dataset. For this reason, I do not identify the subsection below as a formal hypothesis. Obviously, this represents a potential area of future research.

2.7.5.1 The Mass. Data Security Standards are a Form of Traditional Notice-and-Comment Rulemaking

As noted above, the Massachusetts Data Security Standards require the Department of Consumer Affairs and Business Regulation to "adopt [information security] regulations relative to any person that owns or licenses personal information about a resident of the Commonwealth."[167] Similar to the federal Administrative Procedures Act, Massachusetts has a state law that requires "a public hearing [] prior to the adoption, amendment, or repeal of any regulation if [] violation of the regulation is punishable by fine . . ."[168] The enabling statute for the Mass. Data Security Standards permits the Attorney General to bring an action against an offending party for violations of the standards.[169] Massachusetts law provides for fines of up to $5,000 per violation pursuant to such an action if a court finds there have been violations.[170]

[166] *See* MASS. GEN. LAWS ch. 93H, § 2.
[167] MASS. GEN. LAWS ch. 93A § 2(a).
[168] MASS. GEN. LAWS ch. 30A § 2.
[169] *See* MASS. GEN. LAWS ch. 93H § 6.
[170] *See* MASS. GEN. LAWS ch. 93A § 4.

The Mass. Data Security Standards and the Commonwealth's analog to the federal Administrative Procedures Act together create a notice-and-comment rulemaking process similar to that provided for under federal law. Unlike with HIPAA and GLBA, however, the Mass. Data Security Standards do not direct the Department of Consumer Affairs and Business Regulation to give any special deference to industry or other private stakeholders in this rulemaking process. In this regard, the Mass. Data Security Standards are traditional notice-and-comment rulemaking.

2.7.5.2 The Mass. Data Security Standards are Management-Based Regulation Targeting both the Design/Planning and the Implementation Maintenance Stages of the ISPL

The Mass. Data Security Standards are substantially similar both to HIPAA and to the GLBA Interagency Guidelines in specifying both: 1) a general management-regulation style instruction to develop information security plans; and 2) certain details guiding, but not fully directing, the implementation of those plans. The final version of the regulations became effective March 1, 2010[171] and required:[172]

> (1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

This general specification, similar to that in HIPAA and the GLBA Interagency Guidelines (discussed above in Sections 2.7.2.1 and 2.7.3.4, respectively), represents a classic example of management-style regulation. It requires organizations to develop plans to implement broad regulatory goals, leaving substantial discretion to those organizations with respect to their size, scope, and complexity. In this regard, the Mass. Data Security Standards are management-based regulation targeting the Design/Planning stage of the ISPL.

[171] 201 MASS. CODE REGS. 17.05(1).
[172] 201 MASS. CODE REGS. 17.03(1).

The regulations do, however, go on to specify some additional details as to what those information security plans must contain and how they must be implemented. The text of these details is provided in Appendix F.7[173]

As with HIPAA and the GLBA Interagency Guidelines, these regulations are sufficiently directive to interfere at the Implementation/Maintenance stage but lack sufficient detail to justify their characterization as means-based regulation. For this reason, as in the HIPAA and GLBA examples, I suggest that the Mass. Data Security Standards are also management-based regulation targeting the Implementation/Maintenance stage of the ISPL.

2.7.5.3 The Mass. Data Security Standards are Management-Based Regulation Targeting both the Design/Planning and the Output/Efficacy Stages of the ISPL

The Mass. Data Security Standards also have an ongoing evaluation and adjustment requirement similar to that in the FTC's Safeguards Rule and in the FTC's enforcement actions. Consider the requirements in paragraph 2 of Section 17.03 (listed in Appendix F.7), which specifies requirements for the design, update, and maintenance of the security program.

Similar to the analysis in Sections 2.7.3.3 and 2.7.4.1, the requirements to annually review security measures and document responsive actions implicate the Output/Efficacy stage of the ISPL. The similarity among various aspects of these information security regulations is striking, suggesting two possible hypotheses: 1) that regulators so notably lack substantive expertise in this area they feel compelled to draw upon the work of other regulators rather than attempting to innovate in a "federalism experiment" style; and 2) that model of regulation is, in fact, so successful from the viewpoint of regulators and regulated entities that none of these interested parties feel a compelling need to revise it.

2.8 *CONCLUSIONS*

In this Chapter I sought to develop and apply a typology for classifying information security law and regulation. The typology proposed in Section 2.7 is, I believe, an important step forward in understanding information security laws. I make use the classifications discussed in this typology to highlight the differences among models of information security regulation. These classifications allow information security

[173] 201 MASS. CODE REGS. 17.04.

regulations to be grouped together for analysis in ways that permit recognition of why certain conditions result.

Additionally, they identify the subtle, yet important differences among laws that may have future implications for policymakers considering the design of new information security laws and regulations. For example, as discussed above, information security regulators frequently “borrow” from one another. While I have proposed a few hypotheses as to why this borrowing occurs, the similarities among regulations suggest that – in any event – accurate and precise characterizations are important. The subtle, yet crucial, differences between the GLBA Safeguards Rule and the GLBA Interagency Guidelines further highlight the need for a more precise (if more complex) typology for classifying information security regulation.

This classification can help better frame the responses of the Chief Information Security Officers from the qualitative interviews. For example, as discussed in Section 3.9.4.1, the similarities between HIPAA and GLBA may help explain why there was a curious absence of discussion about GLBA in the interviews with CISOs.

Finally, I note that this work does not examine whether the typology I propose is appropriate for or would represent an improvement over current frameworks in evaluating other areas of regulation. It would be a worthwhile exercise to determine if there are other substantive areas of regulation that bear characteristics similar to information security whereby a fine-grained system of classification is appropriate.

3 THE RELATIONSHIP BETWEEN REGULATORY MODELS AND INFORMATION SECURITY PRACTICES

This Chapter discusses a number of findings related to how various forms of regulation differentially affect information security practices at large organizations in the United States. It draws upon both quantitative and qualitative data to examine these differences among the various models of regulation discussed in Chapter 2. In particular, I highlight two key theses of this Chapter with respect to policymaking: 1) organizations subject to management-based "regulatory delegation" models demonstrate a higher capacity to prevent breaches of personal information than do other organizations; and 2) Security Breach Notification laws improve organizations' ability to prevent breaches of personal information even for those organizations previously subject to management-based "regulatory delegation" models.

3.1 INTRODUCTION

As discussed in Chapter 2, there are four major components to information security regulation in the United States:[174 ,175] 1) regulation of information security in the financial sector; 2) regulation of information security in the healthcare sector; 3) state laws of general applicability requiring organizations to notify affected consumers of certain security incidents; and 4) general information security enforcement by the Federal Trade Commission pursuant to its consumer protection (and certain other limited) authority. [176] These components are best grouped into three categories consistent with the classifications described in Chapter 2.

[174] As of the time when this research was conducted; approximately 2007-2009. Since then, as also discussed in Chapter 2, other regulations have been promulgated (e.g., the Mass. Data Security Standards) and other federal legislation has been proposed.

[175] The research conducted for this paper was done before the introduction of Massachusetts' Standards for the Protection of Personal Information of Citizens of the Commonwealth (commonly known as the Massachusetts data security standards). The data sources used in this research, therefore, do not represent consideration of regulation or potential regulation by 17 CMR 27.01. While other states, such as Nevada, Oregon, and California have had "reasonable security" standards in one form or another, however as of time of the last data collection for this research, none of those statutes had yet been enforced in any meaningful form.

[176] There are a variety of other scattered statutes and regulations (e.g., IRS information security regulations, aspects of the Sarbanes-Oxley Act, and state statutes in Minnesota, Nevada, and Washington State mandating various levels of PCI-DSS compliance) not captured in these three broad categories. These categories were selected for the purposes of this research based on their prevalence in affecting organizations' information security practices, their prevalence with respect to publicized information security incidents, and the experience of the author in professional practice.

The first category is industry-specific regulation using a "regulatory delegation" model,[177] which includes in the Health Insurance Portability and Accountability Act[178] ("HIPAA") and the Gramm-Leach-Bliley Act[179] ("GLBA"). While HIPAA and GLBA have some differences between the classification tags applicable to them, they both share the characteristics of being hybrid management-based regulation[180] and are the only two forms of regulatory delegation considered in this research. As discussed above, under the regulatory delegation model, federal legislation requires the development of standards for information security practice and delegates the power to establish and update such standards to administrative agencies. These agencies are directed to seek input from industry through notice-and-comment processes.[181]

The second category is a paradigm in which law requires organizations to report certain types of security failures, potentially linking performance to reputation. This model describes the security breach notification (SBN) laws in effect in most U.S. jurisdictions (see Section 2.7.1 above). Under SBNs, whenever an entity experiences an incident in which certain types of personal information the entity maintains about individuals is compromised, that entity must notify those individuals, a central state authority, local media, and/or other measures. Currently 46 states, Puerto Rico, and the District of Columbia have such laws.

The third category is regulatory enforcement of "reasonable security" standards by consumer protection agencies, most notably the Federal Trade Commission (FTC).[182] The FTC began in the early 2000s bringing enforcement actions against organizations that failed to adhere to their (published) promises[183] regarding privacy and data security measures. Over the course of the last decade, FTC enforcement evolved to focus more on the "reasonableness" of various privacy and data security practices – even absent specific promises about such practices – and the Commission brought enforcement actions based on practices it deemed "unfair."

[177] *See generally* Kenneth A. Bamberger, *Regulation as Deregulation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L. J. 377 (Nov. 2006); *see also* Chapter 4, Section 2.6.2.3.

[178] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 29 U.S.C., and 42 U.S.C.).

[179] Gramm-Leach-Bliley Financial Modernization Act of 1999, Pub. L. 106-122, 113 Stat. 1338 (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.).

[180] *See* Sections 2.7.2 and 2.7.3 above.

[181] I discuss this process, and how it compares to other forms of federal regulation, in Chapter 4, Section 2.6.2.

[182] The FTC has determined it has the authority to enforce certain privacy and data security requirements under its power to challenge unfair or deceptive trade practices. *See* 15 U.S.C. § 45(a)(1); *see also* Chapter 4, Section 2.7.4.

[183] Typically, such promises were those made in "Privacy Policies" published on organizations' public websites.

Currently only two industrial sectors – finance and healthcare – are subject to the first type of regulation. All of the current state statutes comprising the second form of regulation are laws of general applicability and thus, given the highly interstate nature of information exchange, apply to nearly all organizations in the United States.[184] To study the effects of these forms of regulation, I employ a mixed qualitative and quantitative methods approach. I first conducted a series of two-hour semi-structured interviews of Chief Information Security Officers (or functional equivalents) at key U.S. organizations in each of the finance, healthcare, consumer products, energy, and information technology sectors. I then performed analysis on the frequency of reported breach incidents based on data maintained by the Open Security Foundation.

My research and analysis revealed that the various forms of regulation have differential effects on information security practices. Regulatory delegation models encourage collaboration, information sharing, secure information exchange, incorporation of security into system design, and intrusion detection and other perimeter security measures. Laws requiring disclosure of security incidents, in contrast, promote good authentication and provenance, auditing, and host security/internal site security. These disclosure laws also tend to promote the use of encryption for certain sensitive and/or personal information as most such laws exempt incidents from disclosure if the compromised data was encrypted.

The finance and healthcare sectors are each subject to industry-specific regulatory frameworks requiring that they establish practices and standards for information privacy and security. This chapter examines the differences between two categories of organizations: 1) organizations previously subject to management-based regulatory delegation models of information security regulation, which I describe as Previously Regulated Entities (PREs); and 2) organizations not subject to information security regulation prior to the introduction of SBNs, which I describe as Previously Unregulated Entities (PUEs). Additionally, I examine in this chapter the effects that various regulatory models had on specific information security practice areas across all organizations. These goals suggest four primary hypotheses (and one sub-hypothesis):

> **H5: Security breach notification laws linking performance to reputation combined with industry-specific regulatory models incentivize firms to identify risks and employ better security practices than do industry-specific regulatory models alone.**

[184] The applicability of the laws – not accounting for the currently untested question of validity of their long-arm jurisdiction – is determined by the residence of individuals described by the compromised data, *not* by the residence of the organization who was the custodian of the data. Thus an organization resident in New Mexico, for example, which does not currently have a security breach notification statute, could still have notification obligations under the laws of New York State or California if that organization experienced a compromise of data describing residents of New York or California.

H5a: Security breach notification laws linking performance to reputation combined with industry-specific regulatory models incentivize firms to identify risks and employ better security practices than do SBNs alone.

H6: Industry-specific regulatory models incentivize firms to identify risks and employ good security practices even without the presence of SBNs that link performance to reputation.

H7: Security breach notification laws linking performance to reputation encourage the security "practice areas" of access control and operations security in ways that the regulatory delegation process does not.

H8: The regulatory delegation process encourages collaboration and information sharing in ways that breach notification laws linking performance to reputation do not.

I test these four hypotheses using a combination for quantitative and qualitative methods. Specifically, I engage two data sources: 1) quantitative data describing reported security breach incidents since January 1, 2000; and 2) qualitative interviews conducted of Chief Information Security Officers (CISOs) at key large U.S. organizations representing the healthcare, finance, information technology, energy, and consumer products sectors.

3.2 Background Literature

When I began this work, little background literature was available on the subject of "information security regulation." While some scholars have begun to take interest in this area,[185] most of this work is couched in the context of privacy regulation as opposed to information security regulation. The two, while highly related, are critically different for the purposes of my work. Privacy, on the one hand, is inexorably intertwined with normative issues surrounding what choices individuals *should* have regarding the use, tracking, and sharing of their information. Information security, by contrast, can be considered as a purely objective exercise – one aimed at determining the appropriate methods to protect information assets once given (an already accepted and agreed upon) set of normative goals. It is the latter set of questions with which this dissertation is concerned, and thus why I do not provide a lengthy summary of privacy research.

[185] *See, e.g.*, Privacy Law Scholars Conference (PLSC) 2009, http://docs.law.gwu.edu/facweb/dsolove/PLSC/PLSC-2009.htm (last visited Apr. 13, 2011) (noting the substantial lack of papers covering issues of information security). There was a similar distribution of papers at the 2010 PLSC (at which a preliminary version of Chapter 2 of this dissertation was presented), however there is not – as of the time of this writing – a stable URL available for the 2010 conference.

In this section I summarize a 2007 National Research Council Report that served as the initial basis for my dependent variables in considering the "areas" of information security practice I would examine. As discussed in Sections 3.3 and 3.4, it became clear through later work that this report did not fully address all the areas of information security practice appropriate for consideration. Nonetheless, it represents important background and I summarize it in the sections that follow.

I also summarize a March 2010 study by Forrester Research, entitled "The Value of Corporate Secrets." While the publicly available summary report addresses different questions than those addressed in this paper, it does provide some useful background information worthy of inclusion.

3.2.1 The National Research Council 2007 Cybersecurity Report

In 2007, the National Research Council's Committee on Improving Cybersecurity Research in the United States published their findings.[186] This included a ten-provision "Cybersecurity Bill of Rights" which elucidates goals the committee found key to protecting the United States' information infrastructure against both traditional and emerging threats.[187] I examine these provisions in this Section and develop a list of six security "practice areas" (*see* Section 3.3 – Information Security "Practice Areas") to use as "dependent variables" in testing the impact of information security regulation. I begin by considering each provision in terms of the traditional "Confidentiality, Integrity and Availability (CIA)" model.[188] This analysis is conducted in the light of increasing portions of the United States' finance, healthcare, utility and other infrastructures being

[186] National Research Council Committee on Improving Cybersecurity Research in the United States, *Toward a Safer and More Secure Cyberspace* (Seymour E. Goodman and Herbert S. Lin, eds. 2007) *available at:* http://www.nap.edu/catalog/11925.html ("NRC Report").

[187] *Id*. at ES-2 – ES-3, 3-1 – 3-8.

[188] *See, e.g.*, *Information Security*, Wikipedia, http://en.wikipedia.org/wiki/Information_security (last visited Apr. 14, 2008) (providing a basic summary of the CIA model and other derivatives). I note to the reader who may be familiar with the legal practice trend toward specifically *not* referencing Wikipedia that I do so here not for the purpose of serving as an authoritative reference on the subject, but rather to demonstrate the traditional prevalence of this model. Numerous well-written computer security texts are available for the reader interested in a deeper examination of the CIA model, such examination is outside the purposes of this Dissertation.

transitioned to electronic networks operated by the private sector.[189] This analysis is also informed by the results of early interviews with CISOs.[190]

> **1. Availability of system and network resources to legitimate users.** This provision expresses the objective that malicious actors should not be able to interrupt legitimate access to information infrastructure and applications. The most common contemporary threat is the Distributed Denial of Service (DDoS) attack.[191] This provision addresses the availability component of the traditional CIA model. It suggests that there must be focus on the automation of various perimeter security measures and other real-time analytics such as virus and malware protection.
>
> **2. Easy and convenient recovery from successful attacks.** As discussed in the NRC report, this provision addresses not only the obvious case that 100% protection is impossible, but also the broader implications of data erosion and long-term compatibility issues.[192] This provision primarily addresses the availability component of the CIA model, but also touches on the integrity component (particularly in the context of data erosion and long-term compatibility). It suggests that security, particularly disaster recovery, must be taken into account in system design. It also suggests the need for focus on real-time analytics.
>
> **3. Control over and knowledge of one's own computing environment.** This addresses the control that the owner of a resource – whether it be a physical computing device, user account, or network – be aware of all activities occurring on that resource and be able to exercise control over those activities. It is an essential element to successful auditing. This is particularly salient in the context of "botnets"[193] which are a primary component of DDoS attacks. This provision addresses aspects both of the integrity and confidentiality components of the CIA model. It suggests the important of auditing mechanisms and other techniques to

[189] With regard to the first three provisions, the NRC report states that they "relate to holistic systems properties including availability, recoverability, and control of systems" (NRC Report at 3-3) as opposed to "the traditional security properties of confidentiality, authentication . . . and authorization" (*Id*. at 3-4). I find this disambiguation of the CIA model "traditional" and "holistic" classes unsatisfying, and do not follow their separation in my analysis. This concern is further explored below in my discussion of the principles I elected not to adopt from the NRC Report.

[190] *See* Section 3.8 – Qualitative Data Selection

[191] In brief, an threat whereby a single or limited number of users infect many networked machines with code which, when activated, causes these machines to concurrently access a given resource with such volume that the capacity of that resource to serve requests is exceeded rendering the resource inaccessible.

[192] *Id*. at 3-3.

[193] In brief, networked computers compromised by malicious code and the collective actions of such computers driven by this code.

maintain a record of what activities occur on a system. It also suggests that secure and reliable authentication practices are essential.

4. Confidentiality of stored information and information exchange. Much of the transition discussed above in information infrastructures relies upon the exchange of information across public networks including the Internet. Vast amounts of data are maintained by private-sector organizations. This metric is important to ensure such transactions can be conducted in a reliable fashion and that potentially-compromising data[194] is not improperly handled. It addresses the confidentiality and integrity components of the CIA model. It suggests that the ability to safely and securely exchange information among entities over public resources is a necessary element of good security practice.

5. Authentication and provenance. In a networked environment, where transactions are not performed face-to-face, the ability to verify the identity of the application, user, or other entity with whom a resource interacts is crucial. This aspect addresses both the confidentiality and integrity components of the CIA model. This directly indicates the need for secure and reliable authentication practices.

6. The technological capability to exercise fine-grained control over the flow of information in and through systems. Similar to the ability to exercise control over and have knowledge of activities of a resource, the ability to monitor and control the flow of data over networks, computers, and other resources is essential to achieving nearly any potential normative outcome. It is also an essential element of auditing. This provision addresses the confidentiality and integrity components of the CIA model. This further supports the need for real-time analytics and perimeter security systems. It also indicates the need for automation of these systems.

7. Awareness of what security is actually being delivered by a system or component. In order for principals – whether they be users, organizational managers, or technical system administrators – to make implement policy properly, they must be able to discern exactly what a given (technical) security measure does. At the user level, this requires that individuals – regardless of technical experience – are able to make informed decisions about whether or not

[194] e.g., data that can be used to engaged in identity theft.

> an activity violates a stated policy and/or presents a risk.[195] At the (organizational) management level, this requires that key operational and financial decision-makers are making purchasing and policy decisions that will actually reflect their intentions. For system administrators (quite obviously) this requires that the security measures they analyze and implement actually perform the technical functions they expect. This provision, as described in the NRC Report, relates to "crosscutting properties of systems"[196] and as such addresses all three components of the CIA model. It directly indicates the need for auditing mechanisms. It also supports the needs for automation of perimeter security systems and other real-time analysis.

There are three remaining provisions which I do not explicitly consider. The first, "security in using computing directly or indirectly in important applications, including financial, health care, and electoral transactions and real-time remote control of devices what interact with physical processes"[197] is too broad and better describes an outcome than a practice for achieving an outcome.

The second provision I excluded is "the ability to access any source of information (e.g., email, Web page, file) safely." This provision has too much of a normative aspect. I suggest that it is a policy matter, better left to the political system, where we define things like "reasonableness," to determine issues of net neutrality and free speech. The definition of "access safely" is too vague and does not present an objective criterion. This provision therefore does little to help inform the development of security practice areas which can be measured empirically.

The third provision I excluded is "justice for security problems caused by another party." It touches upon concepts such as the ability to assign responsibility for acts in cyberspace, obtain redress, and the technological and legal measures that would be necessary for such goals.[198] These issues, however, are extremely normative in nature and are not properties of an information system, within the control of an organization. Rather, they constitute external elements that influence information security practices.

[195] The most prevalent contemporary case appears to be an inability for home users to distinguish between the purposes and effects of various security software. A recent joint study by McAfee and the National Cyber Security Alliance found that while 87% of U.S. home computer users thought they had anti-virus software installed (94% actually did), only 51% kept that software up-to-date according to industry standards (virus definition files age < 1 week). The same study found that 81% of users had firewall software installed but only 64% had it enabled, and 61% thought they had anti-spam software installed but only 21% actually did. McAfee-NCSA Online Safety Study (Oct. 2007) *available at:* http://staysafeonline.org/pdf/McAfee_NCSA_analysis.pdf.

[196] NRC Report at 3-6.

[197] *Id.*

[198] *Id.* at 3-7.

3.2.2 Utilizing and Improving the NRC Framework

The primary objective of my research is to develop a greater understanding of how to incentivize the people responsible for managing key components[199] of the nation's information infrastructure to make better decisions about their information security practices. This type of evaluation requires the establishment of metrics by which to evaluate if the security decisions they make are desirable. I propose the following framework to describe "good" security practices. It is derived primarily from the needs indicated in my discussion of each of the factors in the NRC report in Section 3.2.1 above. I divide the framework into six information security "practice areas" which, as discussed in Section 3.3, are used as dependent variables to evaluate the effects of various measures on corporate information security practices.

- *incorporation of security into system design*: this concept derives from Item 2 of my distillation of the NRC report ("NRC list") above. It is also generally supported by the remaining seven numbered items I selected as relevant and important to a proposed evaluation framework.

- *secure and reliable authentication practices*: this concept is indicated directly by Item 5 of the NRC list above. It is also supported by Item 3, and indirectly indicated by Items 4 and 7.

- *secure information exchange among public principals*: this concept is directly indicated by Item 4 for the NRC list above.

- *automation of intrusion detection/real-time analysis*: this concept derives from Items 1 and 6 of the NRC list above. It is also further supported by Items 2 and 7.

- *auditing mechanisms*: this concept is indicated directly Item 5 of the NRC list above. It is also supported by Items 3 and 7.

- *collaboration and information sharing*: This category is not explicitly indicated by any of the items in the NRC list above. Rather, it is repeatedly addressed throughout the NRC report[200] and appears to be a necessary category agreed upon

[199] "key components" is defined here primarily as in the private sector.

[200] *See* NRC Report at 39 ("Third, taken together the activities reviewed give an overall sense that—unless we as a society make cybersecurity a priority—IT systems are likely to become overwhelmed by cyberthreats of all kinds and eventually to be limited in their ability to serve society. This future is avoidable, but precluding it requires the *effective coordination and collaboration of private and public sector; continuous, comprehensive, and coordinated research*; and appropriate policies to promote security and deter attackers") (emphasis added).

> by experts in the field. The interview data further support the benefits that information sharing and collaborative efforts are likely to yield.

These six "practice areas" are incorporated into Section 3.3 – Information Security "Practice Areas" – and are described in further detail therein.

3.2.3 March 2010 Forrester Research Report – "The Value of Corporate Secrets"

As described in the Executive Summary to the Report[201], it has four primary goals: "to understand: 1) the value of sensitive information contained in enterprise portfolios; 2) the security controls used to protect this information; 3) the drivers of information security programs; and 4) the cost and impact of enterprise data security incidents."[202] Of these four items, only the third – "the drivers of information security programs" – bears directly on my research. However, each of these items is certainly related and may inform future research work for myself or others. I excerpt a few items from the Forrester Report's "Key Findings" section and discuss the implications of each for my research.

> **Compliance, not security, drives security budgets.** Enterprises devote 80% of their security budgets to two priorities: compliance and securing sensitive corporate information, with the same percentage (about 40%) devoted to each. But secrets comprise 62% of the overall information portfolio's total value while compliance-related custodial data comprises just 38%, a much smaller proportion. This strongly suggests that investments are overweighed toward compliance.

This finding has import for, and is consistent with, my findings with respect to the effects of SBNs (see Section 3.9.4.3) and their effects on the organization and professionalism (see Chapter 4, Section 4.1.2). According to the Report,[203] this result was determined by asking 305 senior-level IT security decision-makers the question: "Please indicate how your IT security budget for 2010 is allocated." The problem with this question is that the response "compliance driven projects and technology," which received 39% of the adjusted budget allocation,[204] may include compliance with initiatives related to

[201] THE VALUE OF CORPORATE SECRETS: HOW COMPLIANCE AND COLLABORATION AFFECT ENTERPRISE PERCEPTIONS OF RISK (Forrester Research, Mar. 2010), *available at* http://www.rsa.com/products/DLP/ar/10844_5415_The_Value_of_Corporate_Secrets.pdf ("Forrester Report").

[202] Forrester Report at 2.

[203] *See Id.* at 7.

[204] The report does not indicate how they adjust, weight, or normalize budget figures across respondent organizations.

compliance with laws not directed specifically at information security, such as Sarbanes-Oxley. As noted in Section 3.9.4.1, the key information security-related provisions in Sarbanes-Oxley are focused on certifying the correctness of information, rather than protecting it from unintended disclosure. While both are valid security goals, the former has a far more limited focus than the scope of my research. It would be interesting to see if it were possible to tease out the differences among specific compliance exercises (e.g., with respect to specific laws/regulations) of that 39% in future research.

> **The more valuable a firm's information, the more incidents it will have.** The "portfolio value" of the information managed by the top quartile of enterprises was 20 times higher than the bottom quartile. These high-value enterprises had four times as many security incidents as low-value firms. High-value firms are not sufficiently protecting data from theft and abuse by third parties. They had six times more data security incidents due to outside parties than low-value firms, even though the number of third parties they work with is only 60% greater.

As discussed in Section 3.7.5, one of the problems with conducting analysis on breach incidence data is that it is difficult to tell whether rises in the absolute number of incidents reported (following the introduction of SBNs) were due to differences in the information security practices of those organizations or to other, unobservable or unquantifiable factors. One of the factors that is unquantifiable (from my dataset) is the "attractiveness" of the firm as a target. The Forrester Report suggests a method of quantifying this "attractiveness" factor, by "divid[ing] the enterprises [they] surveyed into quartiles based on the value of their enterprise information portfolios."[205] While the raw data is not available, it appears one problem with their methodology may be in the way they quantified these values. As explained in the report, "[f]or this survey, we asked respondents to identify the five most valuable assets in their information portfolios out of 17 possible types of information ranging from sales forecasts to cardholder data. For the purposes of simplicity, we constrained the maximum value to $1 million."[206] Firms were permitted to assign values to their data ranging from $50,000 to $1,000,000 for each of the five top assets classes within their organizations. Values lower than $50,000 were discarded.[207] This approach is limited in measuring *relative* value, a key element of determining relative attractiveness of firms – and therefore weighting absolute breach incidence data accordingly – because it requires respondents who may not have training in advanced mathematics to attempt to normalize values when responding. This seems a curious approach, and suggests either that further information on the methodology was left out of the report or that follow-up work to determine if there were greater relative variances is appropriate. In either event, further work in this area could inform deeper analysis into the meaning of the breach incidence data I investigate in Section 3.7.

[205] Forrester Report at 10.
[206] *Id*. at 4.
[207] *Id*. at 15.

3.3 Information Security "Practice Areas"

The following six "practice areas" represents aspects of information security practices I originally sought out to test as dependent variables. As described below, I selected these prior to beginning this research, and conducted interviews with the intent of learning which laws and regulatory schemes incentivized the adoption of various security practices. These areas were partially based on a 2007 cybersecurity report by the National Research Council.[208] As my research continued, I found that these six areas may not necessarily include all the dependent variables for which I should test. Most notably, as indicated in Section 3.9, encryption of portable media appears to be a practice specifically incentivized by SBNs. As described further in Section 3.4, the ten "domains" described in the Certified Information Systems Security Professional (CISSP) industry certification more aptly map to the dependent variables suggested by the qualitative portions of my research. Additionally, as described in further detail below, the CISSP certification is one of the leading professional certifications required of individuals authorized to sign off on regulatory compliance.[209] I do retain, however, some of these practice areas as dependent variables because the CISSP certification does not consider them. Most notably in this regard is collaboration and information sharing, which is not addressed in meaningful form in any of the ten CISSP domains.

I describe below the six areas as they were envisioned prior to conducting the interview portion of my research. The hypotheses in this paper have been restructured from their original form to include the CISSP domains as "dependent variables," rather than using the six areas proposed below. The results are reported according to the CISSP domains, with the exception of information sharing practices. Collaboration and Information Sharing is an area *not* addressed by the CISSP domains, and thus I retain this as a dependent variable for Hypothesis **H8**. The differences between these two approaches (the NRC Report and the CISSP domains) are illustrative of some of the ideas respondents put forth in the interviews as to the importance of various concepts in information security practice.

3.3.1 Incorporation of Security into System Design

This area addresses the extent to which information security issues are considered in the design and implementation of information systems. It can be considered in part as "proactive" security measures, however while most of the practices within this area are

[208] Discussed in Section 3.2.1 above.
[209] *See* Section 3.4.

proactive, this area does not cover all proactive measures. Rather, it specifically focuses on those measures that involve the formalization security considerations into the Software Development Life Cycle and other development and implementation methods.

3.3.2 Secure and Reliable Authentication Practices

This area addresses the extent to which an organization restricts use of its information systems to authenticated users. This area includes all elements of authentication: user accounts, passwords, physical authentication tokens, multi-factor authentication systems, and other authentication practices. It addresses the degree to which these practices ensure that the individual using a system both is authorized to do so and is who they claim to be.

3.3.3 Secure Information Exchange among Public Principals

This area addresses the extent to which an organization ensures that information in transit between and among its information systems and any other systems or uses with which they interact. The primary issue encompassed by this area is encryption, but other issues such as the construction of physical networks can be included.

3.3.4 Automation of Intrusion Detection/Real-Time Analysis

This area addresses the use of real-time tools to protect the confidentiality, integrity, and availability of network resources. It includes analytical tools, perimeter protection tools, data loss prevention tools, anti-virus and other anti-malware tools, and other related automated systems.

3.3.5 Auditing Mechanisms

This area addresses the extent to which an organization ensures that use of its information systems is recorded such that it can be later analyzed. This includes auditing at the operating system level, maintenance of logs of network activity, web server logs, logs of the real-time analytics discussed in Section 3.3.4 above, and any related systems or mechanisms for preserving records or forensic information about the use of information systems.

3.3.6 Collaboration and Information Sharing

This area addresses the extent to which an organization participates in activities designed to exchange information about the types of threats faced by various organizations, security measures employed to mitigate the risk posed by those threats, and other information that may assist in maintaining the confidentiality, integrity, and availability of an organization's information systems. There are special considerations in this area not present in other areas because of the partially competitive nature of information security as an economic good. Some economists have examined this phenomenon,[210] and while full consideration of the issue is outside the scope of this paper it is wroth nothing. For the purposes of this analysis, I consider information sharing to be something that is mutually beneficial to all parties.[211]

3.4 Certified Information Systems Security Professional (CISSP) Domains

The emergence of the CISSP as a (if not the) predominant information security certification in the private sector is in no small part a function of the Federal Trade Commission's privacy and data security enforcement efforts. As early as the turn of the century, the FTC began requiring organizations with whom it entered into consent decrees to agree to regular monitoring of their privacy and/or data security practices.[212] By 2002, these monitoring programs included reports to the Commission that were required to be prepared "by a Certified Information System [sic] Security Professional (CISSP) or by a person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission."[213] Over the course of the next decade, this evolved into a requirement to establish a comprehensive information security program and be subject to regular assessments thereof by a certified security professional.[214] The CISSP certification remains the first certification listed on

[210] *See, e.g.*, Esther Gal-Or and Anindya Ghose, *The Economic Incentives for Sharing Security Information*, 16 INFO. SYSTEMS RESEARCH 186 (Jun. 2005).

[211] I recognize that this assumption is necessarily false in certain situations, particularly with respect to maintaining competitive advantage. Some examples of this condition are examined by Gal-Or and Ghose (2005). However, partial consideration of such circumstances may produce false results and full consideration of these issues is more proper for a behavioral economics paper. For the purposes of this analysis, policies that generally increase information sharing are desirable and therefore this assumption suffices for this paper.

[212] *See, e.g.*, Decision and Order, *In the Matter of Geocities, Inc.*, FTC File No. 982-3015 §§ XII, XIV (Feb. 12, 1999) *available at* http://www.ftc.gov/os/1999/02/9823015.do.htm (requiring respondent to develop an "information practices training program" and to provide reports detailing their compliance with the Order).

[213] *See* Decision and Order, *In the Matter of Microsoft Corp.*, FTC File No. 012-3240 at 3 (Dec. 24, 2002) *available at* http://www.ftc.gov/os/caselist/0123240/microsoftdecision.pdf.

[214] *See, e.g.*, Decision and Order, *In the Matter of Twitter, Inc.*, FTC File No. 092-3093 at 3-4 (Mar. 11, 2011) *available at* http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf (requiring respondent to "establish and implement, and thereafter maintain, a comprehensive information security program . . . " and requiring respondent to "obtain initial and biennial assessments and reports" in connection with its compliance with that program).

the approved list and has been listed first on nearly every consent decree for which certifications were listed by name.[215]

Given the importance of the CISSP certification, at least with respect to FTC compliance, I suggest that its framework presents an excellent means by which to frame dependent variables for testing the effect of regulation on information security practices. As discussed above in Sections 3.2.2 and 3.3, these dependent variables will be particularly useful in presenting the results of the qualitative interviews of Chief Information Security Officers (CISOs). The CISSP certification covers ten areas of knowledge, referred to as "domains."[216] The sections below highlight key summary points describing each domain. I have provided a side-by-side comparison of NRC Report "Practice Areas" and the CISSP Domains in **Appendix E.1**.

3.4.1 Access Control

This domain describes "the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system."[217] It covers those activities related to specifying and enforcing what users of a system can and cannot do. This area overlaps in part with Secure and Reliable Authentication Practices (Section 3.3.2) but is more precise in its specification.

3.4.2 Application Development Security

This domain describes "the controls that are included within systems and applications software and the steps used in their development."[218] It encompasses aspects of the software development lifecycle as it pertains to security, as well as those aspects of software implementation and deployment that relate to security.

3.4.3 Business Continuity and Disaster Recovery Planning

This domain "addresses the preservation of the business in the face of major disruptions to normal business operations. [It] involve[s] the preparation, testing, and updating of specific actions to protect critical business processes from the effect of major system and

[215] *Id.* at 4. *See also generally* FTC Actions, http://www.ftc.gov/os/index.shtml (last visited Mar. 29, 2011) for lists of other FTC consent decrees fitting this description.
[216] *See* CISSP -- Candidate Information Bulletin ("CISSP Bulletin") (Jan. 1, 2009) *available at (via free registration)* https://www.isc2.org/cib/default.aspx.
[217] CISSP Bulletin at 3.
[218] *Id.* at 4.

network failures."[219] Commonly abbreviated BCDR,[220] this domain deals with the security issues involved in maintaining critical operations during a systems failure and with potential attack vectors related to systems failures or the causing thereof.

3.4.4 Cryptography

This domain "addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity."[221] While in practice, the component elements of this domain are highly specific as it relates to cryptography, the description excerpted above is rather broad and in fact addresses explicitly all three of the traditional principles of information security.[222] Additionally, this domain – while specific in its practical focus – actually cuts across two of the six practice areas developed from the NRC Report, including Secure and Reliable Authentication Practices and Secure Information Exchange Among Public Principles. This cross-cutting is an example of when the NRC-based practice areas are not sufficiently well-defined to serve as effective dependent variables.

3.4.5 Information Security Governance and Risk Management

This domain deals with "the identification of an organization's information assets," "documentation and implementation of policies and standards," and "the identification, measurement, control, and minimization of loss associated with uncertain events or risks."[223] While also broad in description, in practice this area deals with documenting, tracking, and managing (physical and information) assets and developing policies and procedures to identify and mitigate risk. It is an area not captured by the practice areas developed from (or addressed in) the NRC Report.

3.4.6 Legal, Regulations, Compliance and Investigations

This domain "addresses computer crime laws and regulations," "investigative measures an techniques," and legal compliance issues.[224] Interestingly, its focus on compliance issues is comparatively small given the substantial attention to compliance activities

[219] *Id.* at 5.

[220] Although, interestingly, not by the International Information Systems Security Certification Consortium ("(ISC)^2"), the organization that maintains and administers the CISSP certification.

[221] CISSP Bulletin at 7.

[222] *See* Section 3.2.1.

[223] CISSP Bulletin at 9.

[224] *Id*. at 11.

identified by the respondents. The primary focus of this area as defined by (ISC)^2 (the CISSP accrediting organization) is investigations, both criminal and civil. It is an area not captured by the practice areas developed from (or addressed in) the NRC Report.

3.4.7 Operations Security

This domain encompasses "controls over hardware, media, and the operators (users) with access privileges to any of these resources."[225] It includes auditing and monitoring activities as they pertain to information resources (but not necessarily, for example, as they pertain to perimeter or network security). This is a fine distinction that provides greater granularity than the NRC Report-derived practice area of Auditing Mechanisms.

3.4.8 Physical (Environmental) Security

This domain "addresses the threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information."[226] This primarily focuses on physical assets/threats such as people, facilities, and equipment, but may also consider other environmental factors such as climate, natural disasters, and military/terrorist threats, particularly in support of other domains such as BCDR. This area is not addressed by the practice areas derived from (nor explicitly mentioned in) the NRC Report.

3.4.9 Security Architecture and Design

This domain "contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, [and] applications."[227] This domain overlaps substantially with the NRC Report-derived practice area of Incorporation of Security Into System design, sufficiently for the purposes of this analysis to consider them equivalent as dependent variables. The domain/practice area can be well-described generally as encompassing issues related to making design decisions and engaging design processes to facilitate and ensure overall system security.

[225] *Id*. at 12.
[226] *Id*. at 13.
[227] *Id*. at 14.

3.4.10 Telecommunications and Network Security

This domain "encompasses the structures, transmission methods, transport formats, and security measures . . . [used] for transmissions over private and public communications networks and media."[228] It deals heavily with issues related to network security and maintenance, perimeter security, intrusion detection/prevention, and secure communications. It overlaps with and can be described as a proper superset of the NRC Report-derived practice area of Automation of Intrusion Detection/Real-Time Analysis. Although broadly-named, the definition of this practice area is more functional for the purposes of a dependent variable as it better matches the types of skills certain individuals have and the types of activities one would attempt to promote with a given area of regulation.

3.5 SCOPE OF INQUIRY

This research began with a focus on traditional "private sector" organizations. As this research evolved, however, it became clear that traditional definitions of public vs. private sector entities – definitions that relied upon the for-profit status of an organization – did 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.[229]

As a result, I expanded the scope of my inquiry 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.[230] Even those states which do not have separate statutes for government organizations make no distinction between for-profit and

[228] *Id.* at 15.

[229] 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. *See* American Recovery and Reinvestment Act of 2009, Division A, Title XIII, Subtitle D (Health Information Technology for Economic and Clinical Health Act), Pub. L. 111-5, 123 Stat. 115 (codified in scatted sections of 42 U.S.C.).

[230] *See, e.g.,* Mass. Gen. Laws ch. 93H, § 3(c) (mandating additional centralized reporting requirements for entities experiencing a security breach if they are state executive branch agencies); *see also* 815 Ill. Comp. Stat. 530/12 (creating separate statutory notification requirements for state agencies experiencing data breaches and requiring additional reporting, including in some cases to consumer reporting agencies).

non-profit organizations. Post-secondary educational institutions, therefore, unlike government institutions, are mostly subject to the same requirements under state breach notification laws as are private firms.[231] Primary and secondary educational institutions, however, are traditionally so interwoven with state and local governments that considering them separately would be difficult. Finally, I include "general" non-profit organizations such as charitable foundations and research institutes. As with private universities and hospitals, non-profits are treated the same under state security breach notification statutes as are private for-profit entities.

I use as my dataset a collection of publicly-known security breach incidents maintained by the Open Security Foundation (OSF) in a database known as the DataLossDB database.[232] As described by the OSF:[233]

> 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.

The database is an open-source effort, similar to Wikipedia, and relies upon the contributions of individuals worldwide to submit known incidents for review. Curiously, the database demonstrates a strong ability to detect even events not yet the subject of public reports – I have encountered incidents listed in the database for which, to the best of my knowledge at the time, the incident had not yet been made public. As of the time of this writing, only limited information as to the methods of collecting information is available.[234] While somewhat detailed, these descriptions lack specificity as to the statistical significance of their sampling methods. As of the time of this writing, I am unaware of anyone having published a study examining this significance.

This lack of specification as to how incidents are captured does present a methodological problem. However, no better resources are available, and for the purposes of preliminary analysis this dataset serves the purpose of allowing analysis on a dataset that at least is likely to exhibit normally distributed error,[235] to the extent error in reporting exists.

[231] 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.

[232] *See* DataLossDB, http://datalossdb.org (last visited Apr. 14, 2011).

[233] *Id*.

[234] *See* About DataLossDB, http://datalossdb.org/about (last visited Apr. 14, 2011).

[235] 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 necessary coincident with when those organizations actually became subject to those obligations. I explore this concept further in the selection of my t_1 and t_2 points as discussed in Section 3.7.2.

Notable limitations worth considering include the incentive for organizations not to disclose incidents that represent breaches of security but escape the technical reporting requirements (e.g., don't 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, I focus only on measuring relative changes over time, an exercise for which properly normalized data – and taking into account the assumption above that any error will be normally distributed – should be sufficient.

3.6 QUANTITATIVE DATA SELECTION

I begin by filtering the dataset for reports which address private organizations in the United States. The DataLossDB database uses a two-level system for categorizing entities experiencing data security breaches. The first, "Sector / Business Type", divides entities into four categories: Business ("Biz"), Educational ("Edu"), Government ("Gov"), and Medical ("Med"). As this study examines private organizations all entries for government institutions are eliminated. As discussed above, for the purposes of this analysis, I treat all post-secondary educational institutions[236] as private firms. For the purposes of this analysis, however, excluding educational institutions as a whole would exclude too many relevant incidents. Furthermore, the volume of incidents at educational institutions makes up a substantial portion (26%) of total incidents in the United States.[237] Additionally, for the purposes of this analysis I treat non-profit organizations[238] the same as private firms.

The second level, "Sector / Business Sub-Type", divides entities into 25 categories which more closely resemble what are traditionally thought of as "industrial sectors."[239] Of these, 18 sub-types cover private-sector entities that fall within the scope of this research.[240] The remaining sub-types correspond to government, educational, and non-

[236] Educational institutions for this analysis are limited to post-secondary institutions. This filtering is accomplished by stripping out all records with Sector / Business Sub-Type of "HS" or "Elem", which correspond to high schools and elementary schools, respectively. There is no separate category for non-elementary grade school.

[237] In the analysis period, there where 2107 incidents within the industrial sectors I examine, with the country designation "US". Of these, 547 involve post-secondary institutions.

[238] Generally, I define this to include organizations recognized under § 501(c)(3) of the IRS code. However, given that the data is somewhat self- and third-party reported, it is possible that other organizations that describe themselves as "non-profit" but that are not officially recognized by the IRS may be included.

[239] *See, e.g.,* 2007 North American Industry Classification System (NAICS) – Updates for 2012, 74 Fed. Reg. 764 (Jan. 7, 2009).

[240]

profit entities. It should be noted that there is not strict sub-typing between the first and second level, and thus is it possible for an entity to fall into the “Biz” type and a “Med” subtype (e.g., a medical device manufacturer).

As of February 17, 2011, the DataLossDB dataset contained 3,076 breach reports from January 1, 2000 through December 31, 2010. 2,575 were experienced by organizations in the United States. Of these, 2,107 fit the criteria described above. 810[241] of these are from regulated industries and the remaining 1297 are from unregulated industries.

3.7 Quantitative Data Analysis

The DataLossDB dataset is freely available for download in comma-delimited and other formats. I downloaded the copy used in my analysis February 17, 2011 and it contains all incidents reported through the DataLossDB website as of that date. This section outlines how I process breach incidence data to analyze the effects of the introduction of state SBNs on corporate security practices.

The dataset is available in comma-delimited (CSV) format. To allow for easier processing, I import the data into a MySQL database table containing rows for each record in the DataLossDB database. I then filter this data according to the criteria discussed in Section 3.6. To analyze trending in breach incidence, I group the incidents into monthly counts according to those in regulated industries and those in unregulated industries. Using a simple java program, I generate a series of SQL “SELECT” and “INSERT” commands which generate a new table with columns for date, number of

Database Identifier Key	Sector / Business Sub-Type
Retail	Retail Businesses
Fin	Financial
Tech	Technology
Med	Medical (Non-Hospital / Provider)
Data	Data Services / Brokerage
Media	Mass Media
Uni	University
Ind	Industry
NFP	Non-profit / Not-for-profit
Org	Organization
Hos	Hospital
Ins	Insurance
Hotel	Hotel
Law	Legal Firm
Edu	Educational
Biz	Business
Pro	Medical Provider
Arg	Agricultural

[241] 354 are from financial sector organizations; 456 are from healthcare sector organizations.

regulated breaches, number of unregulated breaches, and total breaches. Each row represents a single month. The analysis period is January 1, 2000 (t_0) through December 31, 2010 (t_F). I describe the rationale for selecting this t_0 below in Section 3.7.4. Although data is available up through the date of download, the sharply lower number of incidents[242] meeting the analysis criteria described above suggests that all incidents occurring in January 2011 and February 2011 may not yet have been reported. Such a hypothesis is consistent both with the delayed notification provisions[243] of many jurisdictions' SBNs and the reasonable time[244] involved for an organization to consult with the legal counsel regarding a security incident. For these reasons I select December 31, 2010 as t_F (representing the end of the analysis period).

This process resulted in a table tracking the number of breaches reported in each from during the analysis period, separated out by those at PREs and those at PUEs I exported this table in CSV format for analysis to determine an appropriate t_1 (as described in further detail in Section 3.7.4 below). The exported format of this table also provides data for the Microsoft Excel-generated charts used in this section.

3.7.1 Hypotheses tested via Quantitative Analysis (H5 and H6)

As discussed above, I test the following hypothesis (**H5**) using breach incidence data from the DataLossDB database:

> **H5: Security breach notification laws linking performance to reputation combined with industry-specific regulatory models incentivize firms to identify risks and employ better security practices than do industry-specific regulatory models alone.**

I propose to test this hypothesis quantitatively using the two approaches, **Method 1** and **Method 2**, discussed in Section 3.7.3 below. **Method 1** and **Method 2** describe approaches to evaluating the rates-of-change of monthly breach incidence following the introduction of SBNs (t_1) and following the point at which the effect of SBNs reaches saturation (t_2). As discussed in further detail below, the results of analysis using **Method**

[242] Seven incidents in January 2011 and one in February 2011, compared with 24 and 30 the previous January and February and 16 and 25 in November 2010 and December 2010.

[243] *See, e.g.*, N.Y. GEN. BUS. LAW § 899-aa(1)(d)(4) (stating "[t]he notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.").

[244] *See, e.g.*, N.Y. GEN. BUS. LAW §§ 899-aa(1)(d)(2) (stating that "[t]he disclosure [consumer notification] 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 breach and restore the reasonable integrity of the system.").

1 support Hypothesis **H5**. Furthermore, the quantitative analysis reveals evidence suggesting both when SBNs started to have effect and when that effect reached saturation.

Additionally, after completing my research I determined that **Method 2** could have an unanticipated side effect of testing for whether SBNs and industry-specific regulation incentivized better security than just SBNs alone, suggesting the following sub-hypothesis:

> **H5a: Security breach notification laws linking performance to reputation combined with industry-specific regulatory models incentivize firms to identify risks and employ better security practices than do SBNs alone.**

Although my research revealed that **Method 2** was unreliable with the current dataset, I evaluate this hypothesis in the context of the results from that method to suggest possible future avenues for analysis.

I also test the following hypothesis (**H6**) using breach incidence data from the DataLossDB database:

> **H6: Industry-specific regulatory models incentivize firms to identify risks and employ good security practices even without the presence of SBNs that link performance to reputation.**

3.7.2 Key Proposed Time Points (t_1 and t_2)

Testing what effect SBNs have on security practices requires understanding when SBNs became effective. Specifically, I must identify two points: 1) when SBNs first become effective (t_1); and 2) when the effect of SBNs "reaches saturation," or that point at which most firms both are aware of SBNs and are attempting to comply with those statutes requirements (t_2). As discussed in further detail below in Section 3.7.4.1, SBNs neither resemble federal regulation nor traditional state-by-state regulation with respect to these two points. Unlike with federal regulation, there is not one regulation applicable across all U.S. jurisdictions, and thus not a single date or dates[245] (or series of phase-in dates) that can be matched to organizations. Unlike with traditional state-by-state regulation,

[245] In the case of certain regulations, such as GLBA, where multiple federal agencies are responsible for promulgating regulations, there may be multiple dates describing when different organizations comply. These different dates, however, will be clearly linkable to the organizations based on exogenously observable characteristics about those organizations (e.g., in the case of GLBA, what type of financial institution an organization is, and therefore which of the eight GLBA agencies' rules are applicable to that organization).

the applicability of the statute is determined neither by the jurisdictional residence of the organization experiencing the breach nor by the geographical location of the breach itself. Rather, the applicability is determined[246] by the jurisdictional residence of the individuals described in the compromised data, a detail which is neither observable nor inferable from the information available in the DataLossDB database. Given that these two points are not determinable by observable characteristics about the data, this section proposes various methods to derive points that approximate t_1 and t_2 for the purposes of quantitative analysis.

3.7.3 Methods of Analysis

The first method I propose to examine hypotheses **H5** and **H6** is comparing the rate of change of breach incidence during the first six months within enactment of various states' breach notification statutes to rates for the remaining post-enactment periods to the present. I will conduct this analysis for firms within the finance and healthcare sectors and compare the results to the rates of change for all other sectors.[247] My hypothesis (**H6**) that industry-specific information security regulation (HIPAA/GLBA) already was identifying many of the risks that would otherwise have been identified as organizations engaged in SBN compliance efforts – suggests that PREs should experience a smaller drop in breach incidence after t_2 relative to PUEs.

I will supplement this quantitative analysis with qualitative data from the interviews with CISOs. Through analysis of the interviews with CISOs in regulated industries I expect to find that those firms' relatively enhanced ability to identify and protect against threats (i.e., their superior security practices) were linked to the elements of their respective industry-specific laws requiring them to develop security practices and standards. This analysis will also serve the dual purpose of demonstrating that SBNs had an additional positive effect in forcing regulated firms to identify risks and adopt better security practices (**H5**).

[246] Excluding for questions of validity of long-arm jurisdiction, which as of the time of this writing had not been conclusively determined. Furthermore, to the best of my knowledge, as of the time of this writing there had not been any enforcement action brought pursuant to a failure to comply with an SBN, nor had any state attorneys general filed opinions or other guidance as to the long-arm jurisdictional applicability of SBNs.

[247] This analytical approach is derived from one used by Steve Shen and Lorrie Faith Cranor in their paper "An Evaluation of the Effect of US Financial Privacy Legislation Through the Analysis of Privacy Policies."

3.7.3.1 Method 1: Analysis of Rates-of-Change in Breach Incidence After SBNs Reach Saturation Effect (*t_2*)

One approach to testing these hypotheses (**Method 1**) suggests that during the period following the introduction of SBNs, the additive effect of industry-specific regulation will cause PREs to experience less of a drop-off in incident reporting once the effect of SBNs reaches saturation (t_2). I assume that prior to the introduction of SBNs, firms generally would not report security incidents. Following the time at which reporting becomes mandatory (t_1) firms would all experience a jump in reporting rates from some negligible periodic average level[248] R_1 to some level R_2 which will vary according to a variety of factors. One of these factors is the quality of the firm's security practices, for which I am testing. Other factors include the attractiveness of the firm as a target and the amount of sensitive data maintained by the firm. Because these other factors will confound the jump in reporting rates after t_1, comparing these rates may not provide good insight as to the relative quality of security practices between PREs and PUEs. Testing the relative quality of security practices, therefore, requires isolating a variable or trend that depends primarily, if not solely, on the quality of firms' security practices prior to t_1.

Assuming firms have an incentive to report fewer breaches, I can further assume they will take steps to reduce the number of reportable breaches. Such steps would likely include efforts to improve security.[249] Assuming that PREs already will have invested more in security than PUEs, PREs will have less room to improve in this regard and will experience a more shallow drop in incidents after t_2 as they take steps to reduce reporting. This approach assumes that the analysis period is of sufficient length to allow the effects of increased security efforts to be measured across entire industries. During my initial examination, I only used data from January 2000 through August 2009. However, introduction of an additional 16 months of reporting data (the most recent data available as of February 2011) appears to have expanded the analysis period sufficiently to encompass the time required for the effects of increased security efforts to be measurable.

[248] For the purposes of analysis I measure beaches over time with a one-month time unit granularity (essentially reporting and conducting analyses based on how many breaches occur each month).

[249] One possible alternative is that firms will engage greater resources to avoid reporting requirements post-incident. Under an interpretation least favorable to my hypothesis, it seems plausible for certain organizations (particularly those with tighter margins who would have stronger incentive to take the risk (and incur unexpected and perhaps repeated costs later) rather than spend up front), for many – if not most – organizations it seems unlikely to provide a complete solution. Thus it is reasonable to assume that proactive security measures will comprise a significant portion of firms' response to SBNs, even under a least favorable interpretation of corporate behavior. More favorable interpretations – i.e., those that assume firms will behave responsibly in compliance with the spirit of the laws – obviously would further support increased security measures as the response to SBNs.

3.7.3.2 Method 2: Analysis of Rates-of-Change in Breach Incidence After SBNs Become Effective (t_1) and Before SBNs Reach Saturation Effect (t_2)

An alternate approach (**Method 2**) suggests that not all firms will understand or comply with breach notification requirements in a timely fashion. This effect may be further compounded by the extended period over which states adopted such laws. Under this theory, breach incidence may remain steady or increase for an extended period of time following t_1. Again, assuming that PREs will already have invested more in security than PUEs, PREs will be less affected by the increase and will experience a slower rise in incidents as SBNs are adopted and firms move into compliance with reporting guidelines.

I am more skeptical of the efficacy of this approach given that, if we assume t_2 is roughly equivalent for both PREs and PUEs, the efficacy of **Method 2** becomes primarily a function of the overall absolute rise. This is because I expect reporting to be negligible prior to t_1 (both for PREs and PUEs) and I expect both t_1 and t_2 to be roughly equivalent for PREs and for PUEs. The linear rate of change, therefore, for each of PREs and PUEs from t_1 to t_2 will be strictly a function of the absolute rise. As discussed above, in Section 3.7.3.1, there are a variety of factors (such as the attractiveness of organizations as a target and the relative size of those industrial sectors) affecting this absolute rise. If t_1 and t_2 are the same for PREs and PUEs, however, it is difficult (if not impossible) to control for such other factors. Given that I expect t_1 and t_2 to be similar for PREs and PUEs, I therefore do not expect **Method 2** to provide substantial insight. If higher-order polynomial regression analysis reveals substantially a different t_1 and/or t_2 for PREs than for PUEs, **Method 2** might then be more informative.

3.7.3.3 Approximating When SBNs Reached Nationwide Effect and Saturation

Method 1 and **Method 2** are not mutually exclusive, notwithstanding their obvious differences. **Method 2** describes a condition likely to precede **Method 1** in time, and as such if t_2 (or t_1, although I surmise t_2 to be the more likely candidate) differs sufficiently for PREs and PUEs both methods may be informative. If there is a drop-off in breach incidence as a result of firms adopting increased security measures, that drop-off will not likely be measurable until SBNs are in effect and have reached saturation (t_2) in nearly all areas of the U.S.[250] Additionally, the two methods both describe conditions in which the effect of the introduction of SBNs will be less for PREs which presumably will be better equipped to deal with security issues. Given, however, that the efficacy of **Method 2** is

[250] This drop-off may be delayed further if smaller and less technically savvy firms take longer to understand and meet their compliance obligations. However, this factor would likely be adequately captured in regressions of the entire dataset (*see* Appendix A, Section 6.1.1.3) provided sufficient time series data is available to capture the full effect of this delay. Based on the analysis described later in the Chapter, it appears sufficient data is available.

incumbent on sufficiently differing t_2's, a first step will be to quantify t_1 and t_2 both for PREs and for PUEs.

The combination of these two methods proposes a corollary (**Corollary 1**) under which there will exist two inflection points in periodic breach incidence. The first, t_1, describes that time when SBNs begin to affect the decision-making of organizations resulting in those organizations complying with notification requirements. As discussed below in Section 3.7.4.1, given that SBNs were introduced over a period of several years but may affect organizations outside traditional jurisdictional boundaries, it seems likely that there will be an extended rise in incidents after t_1 and before the next inflection point t_2. This next inflection point t_2 describes the point at which periodic breach incidence reporting reaches its local[251] maximum (R_2). Under Hypotheses **H5** and **H6**, this local maximum R_2 at time t_2 represents the point at which breach incidence reporting reaches saturation. Saturation is the point at which no further increase in periodic breach incidence is likely attributable to firms (who had not previously done so) beginning to comply with SBN reporting requirements. My analysis will test for both these inflection points, examining **Corollary 1** in two parts as follows:

> **Corollary 1a:** proposes that there exists an inflection point in the polynomial regression of periodic breach incidence data at some time t_1 representing the point after which firms begin to report security breach incidents with statistical significance. **Corollary 1a** specifically links to **Method 2** for testing hypotheses **H5** and **H6**.
>
> **Corollary 1b:** proposes that there exists an inflection point in the polynomial regression of periodic breach incidence data at some time t_2 representing the point after which generally all firms are aware of and in full compliance with their reporting obligations. **Corollary 1b** specifically ties into **Method 1** for testing hypotheses **H5** and **H6**.

3.7.3.4 Approximation Problems and the Use of Bootstrapping-Like Approaches

Determining over what period to examine the data for **Corollary 1** is problematic. As discussed further in Section 3.7.4 below, there do not exist observable characteristics of the data set indicating when SBNs become effective other than (perhaps) the inflection points and associated changes for which I am testing. Likewise, the data points themselves lack this information due to the structure by which SBNs assert jurisdiction

[251] Although outside the scope of this research because adequate data is not available to create a predictive model for breach incident going forward, I would hypothesize that this is in fact a complete maximum, not just a local maximum. However, for the purposes of investigating these hypotheses, treating t_2 as a local maximum will suffice to analyze the relative rates of change between PREs and PUEs.

over a security breach incident. This is because the data points do not contain information about what individuals' information was described in the data compromised by the security breach.[252] For this reason and others described in greater detail in Section 3.7.4, it is difficult to determine over what period to examine the data to test **Corollary 1**. I therefore propose the solution discussed in Section 3.7.4 acknowledging that it does involve a bootstrapping-like approach of using the data to draw inferences about how to analyze the data. I propose two quantitative approaches, one based on a running averaging model[253] (**Method 3**), and another based on polynomial regressions (orders 2 through 10) over the entire dataset (**Method 4**).

3.7.4 Determining the Appropriate Time Period for Analysis

Perhaps the most challenging part of my analysis was determining over what time period(s) to perform analyses, particularly linear regressions describing the rates of change of breach incidence (for use in evaluating the results of **Method 1** and of **Method 2**). The DataLossDB database includes incidents dating back to August 1903, however coverage before the year 2000 is spotty with most years not even having a single incident. The year 2000 is the first year for which there are incidents fitting my criteria in that year and every subsequent year.[254] Part of the difficulty with this database is that, prior to the introduction of SBNs, firms had little incentive to report breaches on an individual basis. While some limited reporting was suggested under regulations promulgated pursuant to the Gramm-Leach-Bliley Act (GLBA),[255] reporting was not mandatory and did not serve to raise reporting standards to a level sufficient to provide insight into either of Hypothesis **H5** or **H6**. Thus there is not a meaningful baseline from which to establish breach incidence rates prior to the introduction of SBNs, and therefore with which to correlate whether breach incidence increased with increased use of the Internet and other interconnected information systems. For these reasons, I selected to work with data from January 2000 (t_0) onward.

[252] As noted in Section 3.7.3.3 and discussed in further detail in Section 3.7.4.1, neither the jurisdictional residence of the organization experiencing the breach nor the geographic location of the breach event itself determines which (if any) jurisdictions' SBNs apply to the event. The former data point is explicitly defined (or definitely inferable) from the information available in each record in the dataset; the latter data point may be inferable from the information available in each record. However, unlike traditional state-to-state regulation, neither of these conditions applies.

[253] Special thanks to my Qualifying Examination Committee Chair, Yale Braunstein, for his assistance in developing this method.

[254] There are incidents meeting my criteria in 1998, however there was only one in 1999. While I did want to have some data from before the introduction of the first SBN statute, I determined that adding these additional two years of data would unduly bias the higher-order polynomial regressions over the entire dataset as they would introduce too many months with zero incidents.

[255] *See* Determination and Notification of Failure to Meet Safety and Soundness Standards and Request for Compliance Plan, 66 Fed. Reg. 8640 (amending Appendix B § III(c)(1)(g) to 12 C.F.R. Part 570)).

3.7.4.1 When SBNs "Take Effect" – Selecting t_1 and t_2

In selecting periods of analysis for Hypotheses **H5** and **H6**, I need to identify two points t_1 (when SBNs started to affect firms) and t_2 (when SBNs affect reached saturation and all firms generally were affected). Using the DataLossDB data,[256] however, it is impossible to determine "when" a company became subject to SBNs as they are state laws and were enacted over a period of several years. Unlike with most law 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. 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.[257] Thus information about which states' laws would be triggered is completely endogenous to each incident listed in the database.[258] Therefore unlike with traditional state-by-state analysis where one looks to the domicile of a firm to determine if it is affected by regulation it is impossible for the outside observer to make such a determination.

The result is a situation in which measuring what happens "after the introduction of SBNs" is difficult. The most challenging part of comparing the rates of change described above, therefore, is determining an appropriate t_1 to use as the point after which SBNs "affect" organizations. Since, as described above, it is impossible directly to establish this point, I propose the two approaches (**Method 3** and **Method 4**, described in detail in Appendix A) to infer the appropriate period over which to analyze breach incidence for the t_1 and t_2 inflection points.

[256] Nor have I been able to identify any other (unclassified and unprivileged) data sources that could address this question. One possible data source might be billing information from law firms providing counsel on data breach incidents, however this information is protected by attorney-client privilege laws. Furthermore, to reach statistical significance, a substantial amount of this billing information – from many firms – would be required, making it unlikely that a sufficient number of law firms would be able each to convince a sufficient number of clients to allow that information to be released – even in aggregate, anonymized form – so as to render this a workable approach.

[257] 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).

[258] 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.

3.7.4.2 Conclusions Regarding the Appropriate Time Period for Analysis

My analysis[259] of the DataLossDB data suggests clear inflection points in the trend of monthly security breach incidence to use as values for t_1 and t_2. The fact that the candidate t_1 is similar both for PREs and for PUEs is quite interesting, and suggests support for its accuracy. Furthermore, a visual inspection of the other candidate regression curves – both for PREs (*Figure 2a*) and for PUEs (*Figure 2b*) – suggest that the candidate t_1 would be quite similar using polynomial regressions of different orders.[260] Considering these factors, and the limitations of **Method 3** identified in Appendix A, Section 6.1.1.2.3, adopting the suggested candidate t_1 of 56 (corresponding to August 2004) for PREs and the candidate t_1 of 55 (corresponding to July 2004) for PUEs seems preferable to that produced by **Method 3**. Based on this analysis, therefore, it seems reasonable to suggest that an operational estimate of when SBNs began to take effect throughout the United States is between July and August of 2004.

With regard to t_2, regression analysis suggests a slightly broader difference between the candidates for each of PREs and PUEs. Specifically, the (order 5) polynomial regression curve for PREs has a maximum at 105 (corresponding to September 2008), whereas the (order 5) polynomial regression curve for PUEs has a maximum at 102 (corresponding to June 2008). This data suggests a candidate t_2 for PREs at 105, and a candidate t_2 for PUEs at 102. While these two candidate t_2's differ more than do the candidate t_1's, the difference still seems appropriate for the purpose of further analysis. Based on this analysis, it seems reasonable to suggest that an operational estimate of when SBNs reached saturation of compliance was in September 2008 for PREs, and June 2008 for PUEs.

As discussed earlier in Section 3.7.3.2, the efficacy of **Method 2** would depend substantially on whether t_1 and/or t_2 varied substantially between PREs and PUEs. The analysis above suggests that t_1 varies only trivially between these groups. While that analysis does suggest some variance for t_2, the variance appears too small to suggest the efficacy of **Method 2**. As discussed earlier, for **Method 2** to be effective, it must be possible to isolate the relative rate of change in incidents (over t_1 to t_2) between the two groups from the absolute rise in incidents over this period. The only method available to accomplish this separation, given the limitations of the data, is if the periods from t_1 to t_2 vary substantially between PREs and PUEs. Such a condition might allow inferences to be drawn from the rates-of-change in breach incidence across the two groups (over t_1 to

[259] *See* Appendix A.

[260] Assuming that a polynomial of sufficiently high order to handle the entire time series (order > 4) is used, and discounting outliers with unusually high approximations of early negligible activity (e.g., order 5 curves both for PREs and PUEs).

t_2) if those rates differed substantially. However, I do not believe that three months provides sufficient difference to allow for such an approach, therefore I will not endorse **Method 2** as providing insight into either of Hypothesis **H5** or **H6**. Nonetheless, I will run analysis on the period from t_1 to t_2 and report those results to potentially support future research.

Finally, with respect to differences in t_2 between PREs and PUEs, it is worth noting that a sufficiently large difference might in itself suggest something about the differences between PREs and PUEs. Specifically, if the candidate t_2 for PUEs was sufficiently later than that for PREs, it might suggest that PREs had some advantage – as a function of their early regulatory requirements – in complying with the requirements of SBNs. However, as was the case with my analysis above of the efficacy of **Method 2**, I do not believe a two month difference is sufficient to indicate support for such a hypothesis.

3.7.5 Linear Regression Analysis of Trends in Security Breach Incidence

Having identified usable candidates for t_1 and t_2, it becomes possible to analyze the breach incidence data from the DataLossDB database to determine "what happens" after SBNs "take effect" and after SBN compliance reaches saturation. This section will examine these two conditions, following **Method 1** and **Method 2** as outlined in Section 3.7.3 above, to evaluation Hypotheses **H5** and **H6**. It is worth noting that, given the results of the polynomial regressions in Appendix A, Section 6.1.1.3, it seems unlikely that **Method 2** will be usable and thus it will be more difficult to evaluate Hypothesis **H5**. Nonetheless, as noted in that Section, I will proceed with analysis via **Method 2** and report the results with their limitations.

With respect to Hypothesis **H6**, the results of the polynomial regressions suggest that linear regression via **Method 1** will reveal strong support confirming that PREs had an advantage over PUEs in security compliance prior to the introduction of SBNs. If this correlation is as strong as the polynomial regressions suggest it will be, that result would strongly suggest not only the efficacy of HIPAA and GLBA but also that further research be conducted in this area to determine why and how these industry-specific regulations gave PREs a "leg-up" over their previously-unregulated counterparts. I begin exploring such future research through my qualitative data, as described below in Section 3.9 and also suggest questions for future research in Section 3.10.

3.7.5.1 Analysis of Method 1: Linear Regression from t_2 through t_F

As discussed above in Section 3.7.3.1, **Method 1** proposes to test Hypothesis **H6** by evaluating the comparative rates-of-change in monthly breach incidence between PREs and PUEs after SBN compliance reaches saturation (t_2). To accomplish this, I run linear regressions on the monthly breach incidence data after t_2 for each of PREs and PUEs. As with the polynomial regressions, I use the statistical package R, which (under the default configuration) performs linear regressions using the Ordinary Least Squares method. The slopes of the regression lines will indicate the rates-of-change in breach incidence for each of PREs and PUEs.

Unlike with **Method 2**, these rates-of-change will not be dependent on the absolute level (R_2) to which breach incidence reporting spiked at t_2. This is because R_2 represents a saturation level of reporting, or that level of reporting indicative of all the breach incidents occurring with security measures at the time. As discussed earlier in Section 3.7.3.1, I assume that all organizations will have an incentive to reduce the number of breaches they report. There is no evidence to suggest this incentive will vary significantly between PREs and PUEs. Thus the hypothetical target for organizations is a reporting level of zero. However, such a level is unattainable, as "perfect security" is impossible under real-world conditions. Rather, the expected condition is that breach reporting will stabilize at some level consistent with an "acceptable" level of breach incidence. Under this condition, the relative rates-of-change (slopes of the regression lines) will be informative as to the efficacy of security measures existing prior to t_2. If PREs have better security measures prior to t_2, those firms will exhibit a shallower drop-off in breach incidence because they will have "less distance to go" in improving their security measures.

The following chart (*Figure 4*) and *Table 3* depict the results of this regression analysis:

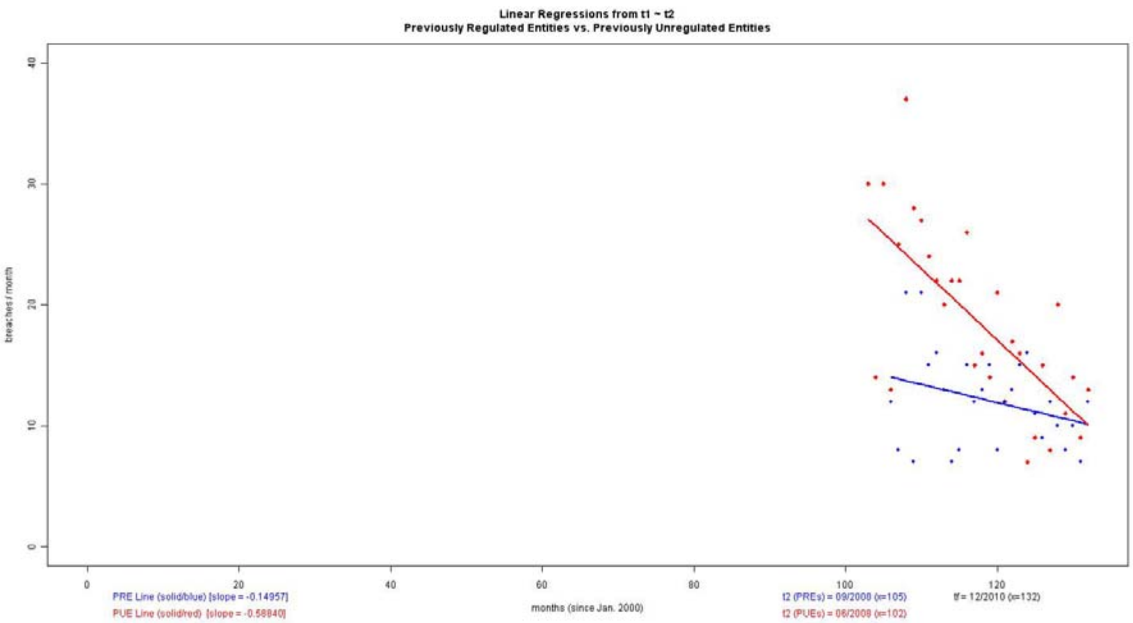


Figure 4 – Linear Regressions of PRE and PUE Breach Incidence from t_2 *to* t_F[261]

[261] A larger version of this chart is included in **Appendix A.6**.

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 3 – Summary of Key Statistical Information from **Method 1** Analysis*

These results strongly indicate that PREs experienced a shallower drop in breach incidence following t_2 than did PUEs. Specifically, the slope of the line describing the drop in breach incidence for PUEs (-0.5884) is nearly four times the slope of the line for PREs (-0.14957). This stark difference suggests that, assuming it is correct that firms across both groups have equal incentive to lower their incidence of breach reporting, PREs had an advantage over PUEs in addressing security issues that result in reportable breach incidents. Such a finding is consistent with and supports Hypothesis **H6**.

3.7.5.1.1 Limitations of Method 1

Method 1 is limited because it rests on the assumption that firms in both group will make equal efforts to reduce their reportable breach incidence after t_2. While it is a reasonable assumption that firms in both groups will have the same incentives to reduce breach incidence, it is not a reasonable assumption that they will have the same capabilities to do so. Thus (under Hypothesis **H5**) while PREs will have less distance to improve after t_2, and therefore should experience a shallower drop in breach incidence, the same "experience" that placed PREs "ahead of the game" may also enable them to correct more rapidly. If they can correct more rapidly, they would therefore demonstrate a sharper drop in breach incidence before reaching some level consistent with their measure of reasonable security.

It is still possible to test for these conditions, although not with the data available as of this time. If my assumption that organizations across both groups will reach some acceptable level of breach incidence consistent with their definition of reasonable security, then the polynomial regression curves describing each group's breach incidence after t_2 will approach some limit R_F which they will reach at some time t_3 (which may be different for each of PREs and PUEs). These regressions would indicate the time it took each group to reach their respective R_F. One hypothesis would suggest that the more rapidly a group reached R_F, regardless of slope of the line describing the decrease in breach incidence from t_2 to t_3. This hypothesis is not inconsistent with the analysis of and conclusions drawn above from **Method 2**, because given the available data, neither industry appears to have reached R_F.

Finally, it is worth nothing that the adjusted R-squared value for the PRE regression line is notably low. This is most likely attributable to the substantial number of outlier months for which there were barely more than five security incidents per month. With the amount of data available at this time, however, there does not appear to be an alterative approach. Interestingly, changing the value of t_2 for PREs slightly (from 105 to 103) alters the slope of the line somewhat (from -0.14957 to -0.19507), but still leaves a substantial relative difference between PREs and PUEs (with PUEs still having nearly three times the slope of PREs). These additional two months brings significance of slope of the regression line for PREs to the 0.05 level. What is even more interesting is that, as noted above in *Table 3* and below in *Table 4*, the slopes of all other regression lines on this data during the analysis period had significance at the 0.001 level.

It is difficult to conclusively interpret these results within the limits of statistical theory, and the conditions described above suggest the importance of further analysis as more data becomes available. Further analysis will reveal both whether this trend continues, and whether the trend will reach statistical significance for PREs. An additional worthwhile exercises might include: 1) examining those outlier months (both negative and positive) to determine if there were any specific events likely to cause outlier conditions; and 2) examination of the actual events reported in outlier months to determine if the events themselves represent outlier conditions that may have biased the data. News coverage of cybersecurity-related incidents increased substantially over the past five years suggesting that the first approach is practicable. The DataLossDB database provides links to primary sources (if available) for each of the incidents recorded in the database suggesting that the second approach is also practicable.

3.7.5.2 Analysis of Method 2: Linear Regression from t_1 through t_2

As discussed at length above in Sections 3.7.4.2 and 3.7.5, the results of the polynomial regression used to select t_1 and t_2 indicate that **Method 2** will not likely be effective at testing whether SBNs combined with industry-specific regulation incentivized organizations to employ better security practices than did industry-specific regulation alone (Hypothesis **H5**). As stated above in those Sections, this ineffectiveness results from an inability to separate the relative rates-of-change between the two groups from the absolute rise in rates from t_1 to t_2. I used the same method of analysis for these linear regressions as that used in **Method 1** and **Method 4**, and report the following results in *Figure 5* and in *Table 4* below:

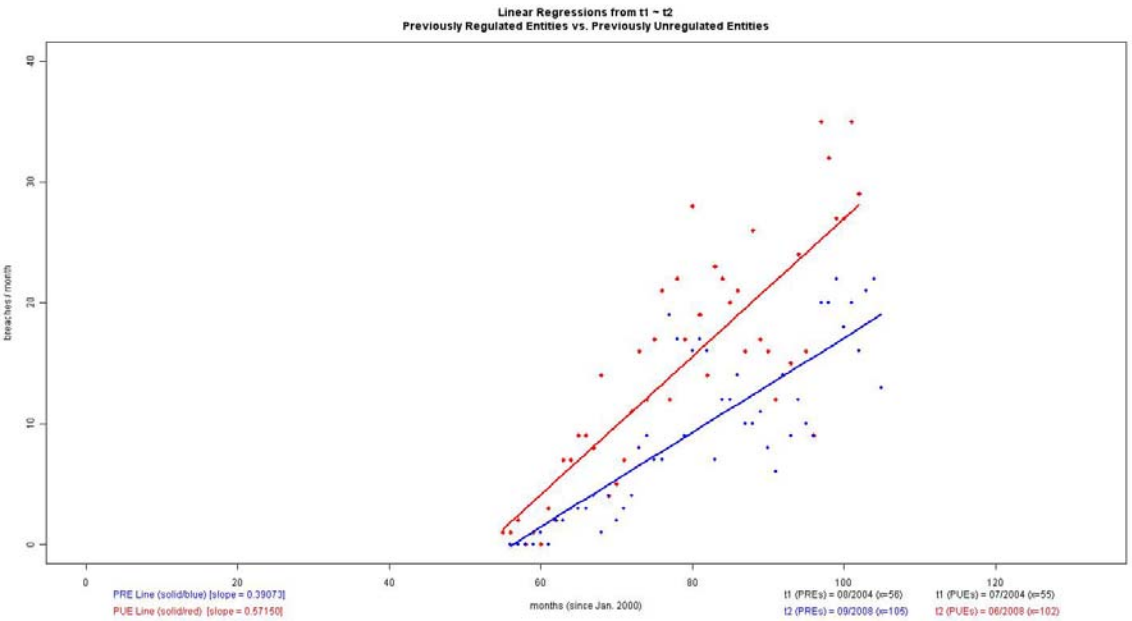


Figure 5 – Linear Regressions of PRE and PUE Breach Incidence from t_1 *to* t_2[262]

Statistical Data	PRE Linear Regression (t_1 to t_2)	PUE Linear Regression (t_1 to t_2)
Residual Std. Error	3.880 (on 48 DF)	5.433 (on 46 DF)
Adj. R-Squared	0.6809	0.6823
p-value	$1.034 * 10^{-14}$	$3.001 * 10^{-13}$
Intercept [sig.]	-21.99395 [***]	-30.17390 [***]
Coefficient x [sig.]	0.39073 [***]	0.57150 [***]
Significance Codes: *** (0.001) ** (0.01) * (0.05) . (0.1) [blank] (1)		

Table 4 – Summary of Key Statistical Information from ***Method 2*** *Analysis*

The data above indicates a slightly sharper (46%) rise in breach incidence for PUEs (0.57150) than for PREs (0.39073). While these regressions have strong significance values and low predicted error, as indicated in the table above, for the reasons discussed in this Section and elsewhere I do not suggest that this result indicates SBNs combined with industry-specific regulation (HIPAA/GLBA) incentivized organizations to employ better security practices than did HIPAA/GLBA alone. Likewise, even though these results would suggest that the combination of HIPAA/GLBA was more effective than were SBNs alone, as apparently evidenced by the slower rate at which breach incidence

[262] A larger version of this chart is included in **Appendix A.5**.

in PREs grew, due to the same limitations I do not suggest that this analysis supports Hypothesis **H5a**.

However, it is worth nothing with respect to Hypothesis **H5** that the fact that there was any significant drop in breach incidence after t_2 suggests that SBNs "added" something to the capabilities of PREs. If industry-specific regulation had been identifying all (or even most) of the primary risks, one might expect breach incidence to rise to R_2 and then stabilize roughly at that level, rather than regularly decrease as suggested by the results in Section 3.7.5.1 above.

3.8 QUALITATIVE DATA SELECTION[263]

My primary qualitative data comprises a series of two-hour semi-structured interviews with Chief Information Security Officers. These interviews were designed to provide insight and intuition about how which 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 hypotheses outlined above.

To select interview subjects I first identified five industrial "sectors" to examine based on the regulatory structures in place at the time of this research (roughly Fall 2007). Based on the existing regulatory structures for healthcare and financial information, I selected healthcare and finance as two of the sectors. I selected energy both based on its being subject to sector-specific regulation more generally, and because of the potential threats emerging with the advent of "Smart Grid" technology.[264] I identified information technology infrastructure[265] as a fourth sector, and consumer products as a fifth. Based on these selections, I proceeded to identify firms that were "major players" in each sector and would be likely to have the greatest knowledge of the security issues facing firms in those industries.

This list led to interviews with nine Chief Information Security Officers representing those firms. These included the CISOs of:

[263] Although this Section is written in the first-person singular, it should be noted that two of my colleagues – Deirdre K. Mulligan and Aaron J. Burstein – participated equally in the design, selection, and conduct of the CISO interviews. It should also be noted that due to technical difficulties during one of the interviews, the results of my interview with the CISO of a major electric utility are not formally reported in this paper.

[264] *See, e.g.*, Smart Grid, http://www.oe.energy.gov/smartgrid.htm (last visited Apr. 14, 2011).

[265] Information technology infrastructure includes those firms that develop or maintain critical elements of information systems that allow global interchange of information. This includes provides of hardware and software for the Internet, operating systems, specific information system applications (e.g., search engines and electronic mail providers), and other similar firms.

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
9. a major provider of healthcare information technology.

3.9 QUALITATIVE DATA ANALYSIS[266]

The data collected from the CISO interviews is sufficiently comprehensive to provide insight into all of my hypotheses. This section presents my preliminary results, including key quotes from interview subjects that exemplify my findings. It further identifies results other than those for which I specifically tested but which are of substantial importance.

3.9.1 Hypotheses H5 and H6

The nature of the responses given by the interviewees suggests that these two hypotheses should be considered together for the purposes of reporting qualitative data.

> **H5: Security breach notification laws linking performance to reputation combined with industry-specific regulatory models incentivize firms to identify risks and employ better security practices than do industry-specific regulatory models alone.**
>
> **H6: Industry-specific regulatory models incentivize firms to identify risks and employ good security practices even without the presence of SBNs that link performance to reputation.**

The first hypothesis suggests that the combination of industry-specific regulation and security breach notification laws (SBNs) will incentivize better overall security practices than SBNs alone. The interviews did not yield a conclusive answer to this question, primarily because the respondents viewed SBNs as interfering with, rather than supplementing, their information security practice. This lack of conclusiveness supports

[266] *See* n. 263.

the need for quantitative analysis as discussed in Section 3.7.1. The second hypothesis suggests that industry-specific regulation will drive good security practices even in the absence of SBNs. The interview data strongly supported this hypothesis. While nearly all the CISOs interviewed indicated that SBNs were a substantial driver of their information security practices, the financial sector respondent did not identify GLBA as a substantially affecting the practices of the respondent's organization. The respondent, however, did identify industry self-regulatory regimes (specifically PCI-DSS) as playing an important role. Respondents in the healthcare field all identified HIPAA as a major consideration in their day-to-day activities, but were mixed as to whether it was the dominant driver of their practices.

One respondent, representing a major financial services provider, did not identify GLBA as having any meaningful impact on the security decisions of their organization. Rather, he identified self-regulatory regimes as having a dominant impact:

> I think in our own industry on driver of the U.S. of late has clearly been PCI,[267] and not that PCI is in any sense mandated externally, because it isn't,[268] data breach notification is kind of external driver, and it's certainly had a change in behavior. And PCI is another one that's had in a sense an almost bigger [effect in] changing actual behavior.

Another respondent, from a large information technology company, mentioned PCI in the context of their organization's overall information security efforts:

> [Compliance with industry standards is] what we expect. . . . if I tell [business partners] that we have PCI and now ISO [17799/2700x] . . . what we've done is . . . we've mapped every compliance requirement and . . . figured out what was common.

Only 3 of the 9 respondents identified PCI-DSS as a driver of their information security programs, and one noted that it only had limited effect.

GLBA does have information security regulations that, among other things, require firms subject to the law to develop and maintain information security plans specifically including lists of salient threats.[269] Yet the respondent failed to indicate that it played any role in their decision-making. I expand further on this in below Section 3.9.4.1. Also notably, as partially indicated above, this respondent indicated that SBNs had a

[267] The respondent here refers to the Payment Card Industry Data Security Standard ("PCI-DSS" or "PCI").
[268] This interview was conducted before any the state statute requiring PCI-DSS compliance took effect. *See* infra Chapter 4, n. 292.
[269] *See* Interagency Guidelines Establishing Information Security Standards, 12 C.F.R .§ 30, App. B § II(A), II(B)(2).

substantial effect on the security practices of their organization. In one example, they stated that:

> Until nine months ago you couldn't have found a single regulator who would say there is [ ] an obligation . . . to encrypt data on laptops. . . . we've gone from a position where it was clearly best practice [to encrypt portable media] to one [where] it's expected by regulators.

Another CISO of a large healthcare organization describes how SBNs had a substantial effect on their organization's practices:

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

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

> . . . what we have done is all computers now have to be encrypted.

In total, 5 of the 9 respondents also identified SBNs as playing a substantial role in driving their information security practices. The fact that SBNs were such an important thread in this interview certainly suggest that they play an important role in driving information security practices. As seen above and in statements by other respondents, SBNs have specifically driven the practice of encrypting devices that contain portable media. While the absence of GLBA from my discussion with this respondent does suggest the need for further empirical investigation, it does not necessarily indicate the law is either ineffective or inconsequential. It may be the case that firms now have sufficient experience complying with GLBA that those requirements have been internalized into industry best practices such that CISOs no longer consider the origin of those practices. It may also be the case that other, stricter standards now dominate the compliance process. This respondent's answers, at least, suggest that PCI-DSS compliance may be one such example.

Respondents in healthcare-industry and related firms all (6 of 9 respondents) identified HIPAA as a major component driving their compliance efforts. One respondent from a major pharmaceutical company described HIPPA as a key regulatory component in their decision-making process:

> . . . [while] we're really operating as business associates under HIPAA so in a sense it's indirect, . . . increasingly folks are just sort of wrapping the HIPAA Security Rule right into the contracts [] themselves. So for all intents and purposes, it's purely like a regulatory component.

He further described their organization as having to "cull out a lot of things [just for] the HIPAA Security Rule."

Another respondent from a large healthcare organization noted how HIPAA had become increasingly important to their organization:

> When [HIPAA] first came around . . . it was very non-prescriptive . . . but now CMS[270] is becoming more specific about how they want to see things. And that's stirring [our compliance activities] up . . .

By contrast, a respondent from a major research university described SBNs as substantially revising the direction their organization took to information security:

> [When I started we were] going to try to figure out the privacy side of it . . . but were also going to build up capabilities to stop the cyber apocalypse because we were worried about that sort of thing after September 11th and also because network security attacks are getting increasingly sophisticated. . . .

Here, the respondent indicates that prior to the passage of SBNs, their organization was thinking differently than after SBNs became effective:

> Then what happened, the Notification Laws came in and said, you don't need to be thinking about that because that's really not that embarrassing. You get hacked, everyone will say, "eh you got hacked. Well that sort of thing happens." Okay, what you really need to be worried about is someone losing a laptop or a backup tape falling off the truck.

The extent to which this respondent was concerned with SBNs was striking given the amount of medical research that occurred in the respondent's organization. Similar to the respondent from the financial services firm, this respondent indicated that industry-specific regulation played a role in their decision-making but that SBNs had become a dominant force.

The central role which SBNs appear to play in respondents' answers makes it difficult to conclude whether the combination of SBNs and industry-specific regulation incentivizes firms to invest in good security practices to a significantly greater than would SBNs alone. However, both the empirical evidence presented in 3.7.5 and the respondents' answers suggest that industry-specific regulation plays an important role in the absence of SBNs, apparently confirming Hypothesis **H6**. The difficulty in providing a conclusive answer to Hypothesis **H5** is that the respondents' answers appear mixed on the degree to

[270] The respondent here refers to the Department of Health and Human Services (HHS) Centers for Medicare and Medicaid services, which at the time of the interviews, was still responsible for enforcement of HIPAA's Privacy and Security Rules. That authority has since been transferred to the HHS Office of Civil Rights. *See* Health Information Privacy, http://www.hhs.gov/ocr/privacy/ (last visited May 5, 2011).

which SBN "compliance" has dominated their decision-making. It certainly seems clear, as indicated by the results supporting Hypothesis **H6**, that industry-specific regulation has *some* effect. The degree to which it will continue to be a driving force is difficult to determine from my analysis to date.

It is worth noting again here that more comprehensive data security regulation, such as the Massachusetts Standards and the recent, more granular data security enforcement by the Federal Trade Commission were not yet a factor when the interviews were conducted. Future analysis on this subject should consider these sources of regulation as well.

3.9.2 Hypothesis H7 – Access Control and Operations Security

> **H7: Security breach notification laws linking performance to reputation encourage the security "practice areas" of access control and operations security in ways that the regulatory delegation process does not.**

This hypothesis suggests that SBNs more strongly encourage authentication and auditing practices than do industry-specific regulations. My interviews revealed that while SBNs may encourage these practices, there is not evidence that they do so to any greater degree than do other forms of regulation. What was most notable about my findings in this regard is that most respondents seemed to view this access control and operations security almost as a "given" in the context of security practices and afforded it little note in their responses. One respondent, for example, representing a major software and internet applications provider, described how their organization's security measures provided extensive information about the identity of users of their services:

> What's amazing is we know so much about each other. . . . I see exactly what they [other CISOs] see. . . . I can see how many federated IDs they use. I can see [] traffic from here to there."

While the quotation above was from a discussion about the respondent's participation in collaboration and information sharing activities, he identified the extent to which they maintain information about the identity of users of their services.

Overall, the respondents had little to say on this subject, which is curious given that all nine respondents identified the concept as being part of their security measures in one form or another. Five respondents did identify a link between HIPAA and these practices, but that link was not well-defined. My research suggests one hypothesis to explain this condition proposing that, similar to the encryption of sensitive information in transit over the public Internet, authentication practices may have become so routine as not to be worthy of significant attention.

Access control and operations security can be expensive practices and while they may help identify the root causes of certain security incidents, they also could subject organizations to additional e-Discovery burdens. As discussed throughout this Dissertation, the Massachusetts data security standards were not in effect at the time these interviews were conducted. The standards do include some logging and auditing requirements[271] and future research into this question may provide further insight.

3.9.3 Industry-Specific Regulatory Delegation Models Encourage Collaboration

> **H8: The regulatory delegation process encourages collaboration and information sharing in ways that breach notification laws linking performance to reputation do not.**

This hypothesis suggests focuses on the "competitive" nature of disclosure-based regulation and the proposition that SBNs may discourage some aspects of information sharing because firms would be incentivized not to share information. If avoiding a breach is a competitive good, SBNs may incentivize firms to withhold information to maintain an information security advantage over peer firms and "stay out of the spotlight." My results were unclear as to whether firms subject to regulatory delegation were more likely to engage in collaborative activities than those not generally subject to such regulation. All nine respondents indicated some participation in collaborative activities, with the strongest interest being expressed by three healthcare organizations, a financial services organization, and a software and internet technologies provider.

Consider, for example, the response of a CISO of a major computer hardware manufacturer:

> "So the only thing we generally won't share is something that I would not want out that could give somebody better ability to attack us and have it work, or would be something that we wouldn't want in the news, because it would create a PR issue."

While it appears that this respondent is supportive of collaborative activities, when asked to elaborate he indicated reluctance to share certain technical details of how various security systems were implemented. This is, of course, the rational response for an individual actor – not to disclose information that could aid an attacker in compromising a system – however, such a position also limits the ability of collaborative activities to become effective. Nonetheless, this respondent did indicate that "there [had] been no data that [he'd] wanted to share that [he] believed was the right thing for the company [] that [he] wasn't able to share." Contrast this response with that of the CISO of a large

[271] *See, e.g.*, 201 MASS. CODE REGS. 17.03(2)(h), 17.04(4).

research university who was responsible for a tremendous amount of Protected Health Information:

> . . . at least among [name of collaborative organization of hospitals] members we all sit there and we compare notes . . . where we basically get together and we chat about security controls and we look at what they're doing to basically stop this and other security breaches along the way . . . we focus on . . . log management, [ ] intrusion protection, all the types of things that would basically help us in what we consider the worst case scenarios . . .

While this respondent does not conclusively state that their organization shares technical detail, their response was far more indicative of confidence in the benefits of collaborative activities. Furthermore, this quote was excerpted from a line of discussion that began with asking about how their organization responded to the compliance-oriented aspects of HIPAA.

Another respondent from a large computer technology firm identified that their organization participated in the Information Technology Information Sharing and Analysis Center (IT-ISCA)[272] specifically because it facilitated information flow both from and to their organization:

> . . . a lot of the [information] will flow through the Information Sharing and Analysis Centers. But I know that [information] flows back into [our organization as well]. . . . we [ ] focus more on those, because . . . there's more bi-directional information flow.

This respondent, however, did not link their organization's information sharing activities to any specific regulatory impetus.

Another respondent at a major financial services firm described information sharing as being abundant in the information security community:

> Yes, so there is quite a lot of knowledge sharing that goes on in the security business, so there is any number of conferences that are generally invitation only, which means that there is a good signal-to-noise ration and [] you are talking to relevant folks. . . . And so I go to two or three of [these] a year and just talk to my colleagues and give presentations on [the subject] . . . those are the kinds of

[272] The IT-ISAC is one of sixteen ISAC's "established by Critical Infrastructure Key Resource (CI/KR) owners and operators to provide comprehensive sector analysis, which is shared within the sector, with other sectors, and with government." *See* National Council of ISACs – About Us, http://www.isaccouncil.org/index.php?option=com_content&view=article&id=87&Itemid=194 (last visited May 5, 2011).

> mechanisms we use, as well as the ISACs[273] are fairly good at sharing information.

Overall, the results were mixed across industries as to whether respondents viewed collaboration and information sharing as worthwhile activities. The quotes above suggest that some healthcare firms have a strong incentive to participate, but as noted above, others expressed reservation and/or little interest in doing so. This remains an open question, one that would be better suited for analysis with a statistically valid sample population.

3.9.4 Additional Key Findings

Perhaps one of the most important findings of my research was to identify what questions the interviews *did not* ask. Searching for this type of information was one of the core reasons for using a small sample size with lengthy, semi-structured interviews. For example, I had expected respondents to talk at length about issues related to FTC enforcement, and yet only one respondent even mentioned the FTC (and perhaps because that respondent's organization was currently under an FTC consent order).[274]

3.9.4.1 Absence of Gramm-Leach-Bliley in Discussions with Respondents

The Gramm-Leach-Bliley Act (GLBA) and its implementing regulations prescribe a variety of information security requirements for firms subject to the jurisdiction of the regulatory agencies responsible for implementing GLBA. I examine GLBA and its implementing regulations in detail in Chapter 2, Section 2.7.3. What was particularly notable about the CISOs' responses is that *none* of them identified GLBA as a driving force for their information security practices. The one respondent from the financial services industry did not even mention GLBA, and the only two respondents that mentioned it only did so in passing and both indicated that it did not enter into their information security calculus.

[273] Here the respondent is referring to Information Sharing and Analysis Centers, *see generally* http://www.isaccouncil.org/.

[274] Several respondents did reference "TX Maxx", "Choicepoint", or "BJ's" (presumably referencing the FTC consent orders/settlements with those respective organizations) as undesirable events that may have contributed to their organization's increased focus on information security. However, these were all references made in passing conversation and lacked any further linkage to potential future activities by the Commission. Rather, it appeared that the CISOs I interviewed were more considered about the media repercussions of such an event than an investigation by the FTC's Bureau of Consumer Protection.

Two possible hypotheses could explain this result. First, the agencies with the authority to enforce GLBA and its implementing regulations had not yet engaged in substantial enforcement as of the time of the interviews that would have been noticeable to the respondents. While this does not exclude the possibility that regulators engaged in informal enforcement, none of the Department of the Treasury agencies have engaged in any formal enforcement actions. By contrast, the Federal Trade Commission *has* engaged in enforcement actions based on its GLBA Safeguards Rule as far back as 2004.[275] It is unclear from the interview data whether this FTC enforcement would have been noticeable to the respondents, however the resultant consent decrees did require the implementation of comprehensive information security programs and biennial audits for the subjects of the enforcement actions.[276] Further research in this area is warranted to investigate the effect of GLBA on information security practices.

Second, it is possible that other compliance activities – notably those for HIPAA, which would apply to 6 of the 9 respondents – would be sufficient to meet the requirements of GLBA and thus the attorneys involved in the compliance certification process may have "re-used" the compliance plans from HIPAA for GLBA-related activities. As discussed in Chapter 2, HIPAA and GLBA are remarkable similar in that both the HIPAA Security Rule and the GLBA Interagency Guidelines are forms of management-based regulatory delegation targeting both the design/planning and implementation/maintenance stages of the ISPL. This similarity suggests that compliance officers might be inclined to "re-use" security plans from HIPAA for GLBA compliance purposes. While the FTC Safeguards Rule differs in that it targets the output/efficacy stage rather than the implementation/maintenance stage, this is a technical distinction that might escape a non-technical compliance officer and result in "re-use." Further research to investigate this question could include a more structured survey of respondent CISOs that specifically asked this question. Additionally, it would be informative to include among the respondents attorneys involved with each organization's compliance activities.

[275] *See, e.g.,* Complaint, *In the Matter of Sunbelt Lending Servs., Inc.*, FTC File No. 042-3153 (Nov. 16, 2004) *available at* http://www.ftc.gov/os/caselist/0423153/041116cmp0423153.pdf; *see also, e.g.,* Complaint, *In the Matter of Nationwide Mortgage Group, Inc.*, FTC File No. 042-3104 (Nov. 9, 2004) *available at* http://www.ftc.gov/os/adjpro/d9319/041116cmp0423104.pdf.

[276] *See, e.g.,* Agreement Containing Consent Order, *In the Matter of Sunbelt Lending Servs, Inc.*, FTC File No. 042-3153 (Nov. 16, 2004) *available at* http://www.ftc.gov/os/caselist/0423153/041116agree0423153.pdf, *see also, e.g.,* Agreement Containing Consent Order, *In the Matter of Nationwide Mortgage Group, Inc.*, FTC File No. 042-3104 (Mar. 4, 2005) *available at* http://www.ftc.gov/os/adjpro/d9319/050304agreeconorder.pdf.

3.9.4.2 Absence of Sarbanes-Oxley (SOX) as a Force Driving Information Security Practices

One of the original assumptions was that respondents would spend a substantial amount of time talking about compliance with the Sarbanes-Oxley Act of 2002.[277] In particular, I expected that the § 404 "internal control report" provisions of the Act would have driven firms to invest substantially in information security compliance efforts aimed at certifying compliance of their internal controls over financial reporting. While four of the nine respondents mentioned SOX, most mentioned it only in passing, reported having minimal involvement in it, or described it as an exercise in "certification, not security."

Only one respondent reported any meaningful involvement with SOX compliance. Notably, this was the respondent who represented a major financial services company. He remarked that:

> . . . we then all live in the SOX-404 world where we have this huge complicated SOX management program, and IT actually bears a chuck of responsibility for managing the [] controls for [organization name] under SOX . . . .

This respondent described SOX as "too prescriptive around the kinds of control you need and therefore incurs costs where you have [to] test the controls that don't necessarily actually do much." This aspect of regulation, where compliance drives information security efforts – as opposed to the "risk management approach" the respondents favored nearly unilaterally – was also discussed by the respondents in the context of breach notification laws forcing them to encrypt all their devices. Ironically, the subject above then proceeded to observe that:

> despite my reservations about [CA 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, it was like one paragraph.

This last observation was in stark contrast to nearly all of the other respondents, who reported that "compliance" with SBNs (specifically, encrypting portable media to avoid reporting loss of devices) *distracted* them from their primary tasks of protecting the organization's information from abuse.

[277] Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745 (July 30, 2002) (codified as amended in scattered sections of 15 U.S.C., 18 U.S.C., and 28 U.S.C.).

3.9.4.3 Security Breach Notification Laws Drive Encryption of Portable Media

Perhaps not surprisingly, the “encryption exception” present in most states’ SBNs – whereby the loss of control of portable media does not need to be reported to the affected individuals if the data contained on that media was encrypted – has driven substantial efforts on the part of organizations to encrypt their portable devices. What is perhaps surprising, however, is that not all the CISOs I interviewed saw this as a good thing from a security perspective. Furthermore, it did not necessarily drive the encryption of all devices/connections – just those that resulted in events requiring reporting under SBNs. In total, five of the nine respondents identified SBNs as a driving force for encrypting at least some devices and/or data.

Consider the response of one CISO, also examined above, in the context of the efficacy of SBNs at improving the security of their organization:

> What little evidence that we have in terms of the actual harm from these things comes principally from the kinds of things where it actually gets in the wrong people’s hands, who can actually use it. . . . And so [] basically it has distracted us from [] what I think is [the] important thing . . . to build up the security capacity to actually address things like botnets and really significant network security vulnerabilities that we have. We have a very difficult time closing all our vulnerabilities. . . . This whole crypto business that we’ve been under has essentially moved resources from that area which we were kind of focusing on to this other area. . . . And so it’s not as if every dollar that I spend on crypto is a dollar I don’t get to spend on something else . . .

This respondent clearly believes that SBNs serve to direct their efforts away from more critical priorities, and that by taking up a substantial portion of their resources efforts to avoid notification events have reduced their ability to protect their organization’s information assets. The respondent cites the negative media appearance of losing portable media as being the primary driver of these efforts:

> . . . what you really need to be worried about is someone losing a laptop or a backup tape falling off the truck. That[] . . . makes your organization [look] a lot more incompetent. If you got hacked by some sophisticated hacker, well, you know, that’s the sort of thing that happens. If you lose a backup tape or somebody gets a laptop lost, well that’s stupid. No one likes to be seen as stupid.

Another CISO of a large computer technology firm describes the difference between the common perceptions of (consumer) data protection requirements as different from the actual steps necessary to successfully protect that data:

> Everybody thinks you should just encrypt [information], [be]cause then you got your data protection and “problem solved.” And it’s honestly not that easy . . . .

> you’ve got to think through . . . [in different conditions whether] you [are] actually getting the encryption or not in those [conditions].

This CISO’s observation about what “everyone thinks” resulted from the encryption “safe harbor” provisions in the SBNs.

Other respondents, with the notable exception of the CISO of the major financial services firm (discussed above), reported similar attitudes toward SBNs. Their criticism seemed to stem from their opinion that events like the loss of portable media – an event they viewed as being one of the predominant SBN-triggering events – were *unlikely* to actually compromise the security of their data. The CISO quoted in this section went on to say:

> There’s not much reflection on whether or not anyone ever uses that data. It’s still a breach. It’s still a compromise because some hobo stole it, stole a laptop with a bunch of information on it and turns around and sells it to a pawn shop . . . . That’s the sort of the model that the use. It’s nuts because the actual attacks, network attacks are likely to be much more damaging. Somebody might actually use the data.

In many ways, this quote exemplifies the finding of this section – the encryption “safe harbor” provisions in the SBNs create a compliance-like atmosphere where security efforts are aimed at avoiding a negative event (the public event of breach notification) without respect to whether actual harm through abuse of the compromised data was likely to result. It is important to note here that many states’ SBNs have “risk of harm” standards, whereby if after an investigation a data custodian reasonably believes that the data is unlikely to be used for identity theft or other criminal purposes, the breach does not need to be reported. However, it appears that at least in the opinion of this CISO, meeting that standard is difficult and its presence does not alter the “compliance” efforts their organization forces the respondent to undertake.

3.9.4.4 Incorporation of Security Into System Design

This was a topic that most of the respondents did not directly address. All nine of the respondents identified it, however only three addressed it directly and only one linked it to regulatory requirements (HIPAA). Consider the response of the CISO of a major software and internet applications company, who indicated that security review was an integral part of the software development process at their firm:

> [Security] is in multiple stages. In some cases we can find out about the problem right before they want to release [the software] . . . that is the integrity layer of the system so everything that does in appears to be checked [and has to show] no vulnerabilities. Beta [software, by contrast] can come out but betas have to come out in certain settings [designed to protect security] . . . . the final security review

> is where [] you jump from that so-called alpha, [to a] beta [that is] somewhat secure[, and then] into full production.

It was clear that, at least in the case of this respondent's organization, the incorporation of security into system design was a top priority. The respondent described their department as a "tax" on other departments – they had to pay the tax (i.e., allow the respondent's team to perform their functions and grant approvals) – before production could advance.

Consider the response of the CISO of a large financial services organization while discussing the issue of (access) privilege accretion:

> And so it's important to make sure that the architectures are well constructed . . . that they have considered the security threats and that they are [ ] uniformly implemented . . . .

For this CISO, security was an essential part of the software development process to ensure that, over time, users would not accrue greater privileges than they should. This CISO also noted particular concern with making sure that:

> projects can't just scuttle off and do something that [ ] undercuts your architecture and subverts [ ] your security controls just because they feel like it and nobody ever reviewed [the project].

What was unclear from the interviews was if this process was the result of any specific legislative activity. This is an area I suggest for further research as it often can be the weak point in an organization's security measures.

3.10 FURTHER RESEARCH

The quantitative work discussed in this Chapter is descriptive, not predictive. Quite obviously, the linear regressions outlined in Section 3.7.5.1 (from t_2 to t_F) will neither approach zero nor become negative. As more data becomes available, it may become possible to use additional polynomial regression modeling – over only the later parts of the dataset – to identify a third inflection point t_3, after which breach incidence starts to "level-off" toward some sustainable level. This may enable the model to serve predictive purposes, beginning with a stable level of breach incidence and possibly, with enough (external) historical data, predictions considering how breach incidence levels will react given changes in external factors such as regulation, significant (worldwide) security failures, or significant law enforcement victories (e.g., the dismantling of a large organized crime organization with substantial resources dedicated to electronic crime).

Developing a predictive model, or at least analyzing enough data to determine where such "leveling-off" will occur has important implications. "Leveling-off," or the rate of breaches per unit time at which each of PREs and PUEs stabilizes, will necessarily happen (absent other confounding events) because the rates cannot continue to decrease below zero. When there is sufficient data to determine the time(s) (t_3's) at which this will occur, determining whether the rates are similar for PREs and PUEs will provide significant information for policymakers. If the rates are similar, it will suggest that while management-based regulatory delegation models enable organizations to implement procedures to prevent breaches of personal information more quickly, both models of regulation will achieve an equal result in this regard given sufficient time. If PREs stabilize at a lower level (relative to PREs' peak at t_2) than the level at which PUEs stabilize (relative to PUEs' peak at t_2), this will suggest that management-based regulatory delegation models provide an additional capacity at preventing breaches of personal information that SBNs do not. Conversely, if PUEs stabilize at a lower level than to PREs (each relative to their respective peaks at t_2), this would suggest the curious condition that over the long term, management-based regulatory delegation may inhibit the capacity of organizations to prevent breaches of personal information.

Current trends do not suggest which of these conditions will be correct, however the relative rates of decrease in breach incidence discussed in Section 3.7.5 suggest that the third condition will not result. It remains unclear at this point which of the first two conditions will be correct. The existing data suggest that at least an additional six months of data will be necessary before reaching any conclusions. It is also unclear what methodology will be successful in determining a t_3 to describe these "leveling-off" points, however it seems likely some form of polynomial regression analysis (see Appendix A) will be appropriate.

Additionally, the method of sampling I used for grouping breach incidents normalized the data according to calendar months (effectively running a one month simple moving average with a sampling frequency of one month). While the polynomial regressions I ran should account for any frequency sampling issues, it would be interesting to re-run the analysis using different simple moving average periods and different sampling frequencies. While I do not expect such an approach to alter the results in terms of my conclusions, it could potentially increase the significance of the coefficients in the linear regressions if, as I suspect, the one regression coefficient with a lack of significance is due to a few outlier months just after t_2 for that industry group.

Finally, although perhaps obvious, it is worth noting that the qualitative sampling size is both small and heavily biased toward healthcare-related industries. My data suggest two potentially worthwhile exercises as follow-on to this research. First, it suggests conducting more concise interviews with CISOs of several more organizations – particularly in the financial services sector, where I had the least number of respondents. Second, my results suggest conducting statistically-valid surveys of CISOs (or functional equivalents) at U.S. organizations to tell certain precise hypothesis that have emerged from this research.

3.11 Conclusions

This Chapter examines the differential effects various models of information security regulation have on large organizations' security practices in the United States. As discussed in the Introduction, the quantitative data suggest two key findings in this regard. Additionally, the qualitative data revealed some surprising findings suggesting the importance of conducting future quantitative work to test the effects of certain laws on information security practices.

The quantitative data first suggest that management-based regulatory delegation models, such as those present in HIPAA and GLBA, result in organizations in the finance and healthcare sectors having greater ability to prevent breaches of personal information than do other organizations. This finding has two important policy implications. First, it suggests that these management-based regulatory delegations models have a broad-based effect of improving information security practices in organizations. Preventing breaches of personal information in the manner sought by SBNs was not an original intent of either HIPAA or GLBA.[278] Rather, these regulatory frameworks impose broad obligations on organizations to implement and adhere to information security plans conforming to a range of general security goals. Nonetheless, the quantitative data strongly suggest that these organizations exhibited significantly greater capacity to reduce breaches of personal information. This finding suggests the efficacy of such models of regulation. This result also suggests a second important finding that engaging in broad security principles increases an organization's ability to later implement a specific security practice. While not conclusive on all permutations of this finding (i.e., it only tested the "specific security practice" of avoiding breaches of personal information), it does provide empirical evidence that – in practice – good overall security measures do increase organizations' capacities to prevent specific security failures not explicitly addressed in their overall security plans. If this conclusion is true more generally, it suggests to the policymaker that broad, management-based regulatory delegation models may be an effective prophylactic measure to mitigate a broad range of security risks – particularly in cases where not all the security risks are known *a priori* the legislation.

The quantitative data also suggest that SBNs are effective at improving organizations' capacity to prevent breaches of personal information even when organizations are already subject to management-based regulatory delegation models of information security regulation. This finding is important for policymakers considering layering a breach notification requirement onto existing regulation. It suggests, for example, that the

[278] The HITECH Act provides a breach notification requirement for healthcare industry organizations, however it was not passed until 2009 and did not alter this analysis because nearly all such organizations were already required to report breaches under state SBNs. *See* American Recovery and Reinvestment Act of 2009, Division A, Title XIII, Subtitle D (Health Information Technology for Economic and Clinical Health Act), Pub. L. 111-5, 123 Stat. 115 § 14302 (codified in scatted sections of 42 U.S.C.).

decision to include a breach notification requirement in the HITECH Act's revisions to HIPAA was the correct choice to improve healthcare organizations' capacity to prevent breaches of personal information. It also suggests, for example, that the European Union (which does not currently have a breach notification requirement) may wish to consider implementing such a requirement if regulators are concerned about organizations' existing capabilities to prevent breaches of personal information.

The qualitative data suggested a few additional conclusions worthy of note. First, the absence of discussion of GLBA by the respondents is a curious result. In Section 3.9.4.1 I suggest a few hypotheses as to why this may have been the case. In any event, the contrast here between the qualitative and quantitative data as to the importance of GLBA suggests that further investigation is warranted into its effects. Second, the qualitative interviews suggest that Sarbanes-Oxley is not a major driver of information security practices. As discussed in Section 3.9.4.2, this appears to be the result of SOX's focus on certification as opposed to security more generally.

4 The Differential Effects of Information Security Regulation on Professionalism in Large Organizations

4.1 Effects on the Organization

In Chapter 2, I characterize the various regulatory structures governing information security in the United States. This Chapter identifies how certain of those characteristics result in conditions that have substantial import for how organizations relate to and employ the services of information security professionals. I again draw upon the CISO interviews as an empirical data source to illuminate the discussion in this section. I focus on two opposing forces generated by regulation, one that encourages reliance upon the discretion of information security professionals and another that establishes "absolute" standards which interfere with the exercise of professional discretion by information security professionals. Each of these corresponds to certain of the regulatory structures discussed in Section 2.7 above.

4.1.1 Regulation that Encourages Reliance on Professional Discretion

Understanding the differences between HIPAA and GLBA rulemaking and traditional notice-and-comment rulemaking under the APA sets the groundwork to explore the implications of this difference for the exercise of professional discretion within the organization. I then consider this distinction in conjunction with management-based regulatory delegation aspects[279] of HIPAA, GLBA, and FTC enforcement described above in Sections 2.7.2, 2.7.3, and 2.7.4 respectively. The following hypotheses result:

> **Hypothesis H9: regulation that relies upon industry for the development of specific standards or rules (forms of management-based regulatory delegation) strengthens the role of information security professionals within organizations.**
>
> **Hypothesis H9a: regulation that specifies or requires deference to industry in the rulemaking process necessitates reliance on the professional discretion**

[279] As noted above in these respective sections, not all aspects of these regulatory regimes – particularly of FTC enforcement – are management-based in style. The distinctions laid out earlier in Sections 2.5 and 2.6 are informative here because they help illuminate why regulations like HIPAA, GLBA, and FTC privacy and data security enforcement – which on the surface bear similarity to regulatory regimes like food safety, pollution, consumer notification, and other more "traditional" regulations – must be considered differently in terms of their effect on the organization.

and judgment of information security professionals for participation in the rulemaking process.

Hypothesis H9b: regulation that requirements firms to develop (and adhere to) standards of "reasonable security" (management-based regulation) necessitates reliance on the professional discretion and judgment of information security professionals to define what are "reasonable" security practices for the organization.

The overarching hypothesis of this section is that regulatory structures like HIPAA, GLBA, and FTC enforcement enhance professionalism in the information security space. They do so by requiring regulators and organizations, through the various means outlined above in Hypotheses **H9a** and **H9b**, to rely more heavily on the input of information security professionals. Professionals' input, therefore, is required to advance organizations' interests with respect to regulatory goals. Thus those organizations – and therefore the senior managers therein – will need to defer to the professional discretion and judgment of information security professionals.[280]

Professionals serve two roles in this regard: 1) they serve to reduce uncertainty for decision-makers in senior management; and 2) they inform decisions as to mitigating risk. In the sections that follow, I examine each of these roles in the context of information security professionals using the CISO interviews as primary data and also consider prior research conducted on the role of Chief Privacy Officers (CPOs)[281] as an empirical backdrop. The first role and the regulatory structures that enable it drive the second role – in an environment where compliance failures are both costly in regulatory violations and in public exposure,[282] the need is high for organizations to mitigate risk to avoid incidents likely to result in regulatory action and/or media coverage.

[280] *See* infra n. 286.

[281] *See* infra n. 286.

[282] The follow are examples of coverage of the FTC's investigation of Twitter, Inc. (*see* Decision and Order, *In the Matter of Twitter, Inc.*, FTC File No. 092-3093 (Mar. 11, 2011) *available at* http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf). All of these represent major, widely-circulated print and electronic publications covering the information technology industry. A simple Google search (conducted Apr. 9, 2011) using the search terms "ftc", "investigate", and "twitter" revealed these as the top results. Note that many of the articles were published only within hours of the FTC's press release.
http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=229301037
http://www.macworld.com/article/158509/2011/03/twitter_settlement.html
http://www.networkworld.com/news/2011/031111-ftc-officially-closes-twitter-security.html
http://www.computerworld.com/s/article/9214238/FTC_officially_closes_Twitter_security_investigation
http://www.pcworld.com/businesscenter/article/221961/ftc_officially_closes_twitter_security_investigation.html
http://www.cio.com/article/676213/FTC_Officially_Closes_Twitter_Security_Investigation

4.1.1.1 Information Security Professionals Reduce Uncertainty in an Uncertain Regulatory Environment

Two characteristics about the regulatory environment created by HIPAA, GLBA, and FTC enforcement create the need for organizations to rely on information security professionals. First, the need to participate in the rulemaking process for regulations like HIPAA and GLBA, as described in Section 2.6.2.3 above, requires the involvement of information security professionals. Second, information security professionals must exercise their judgment as to the mechanics of compliance with regulations, particularly ones predicated on concepts of "reasonableness." This section discusses the first characteristic. I discuss the second characteristic in Section 4.1.1.2 below.

Even without Congress's command, organizations have a strong incentive to participate in the rulemaking process whenever possible. When agencies conduct rulemaking, those organizations who participate in the process will have a decided advantage over those that do not. This is because in complex regulatory regimes, risk is highly individualized and heterogeneous among organizations.[283] Bamberger (2006) describes how "[o]ne-size-fits-all rules cannot easily account for the ways in which manifests itself differently across firms."[284] In an environment like this, organizations are strongly incentivized to participate in the rulemaking process so that their views will be represented in the resultant regulations. Incentives to participate are strengthened when Congress commands the rulemaking authority to consult industry, because in those cases there necessarily will be industry participants and those who do not participate (or are unrepresented in the process) will necessarily be disadvantaged.

Consider the responses on one CISO, when discussing the role of regulators with respect to information security rulemaking:

> [M]y experience with regulators is that if they're not [technical] systems people and they're not really in a position to [(learn the technology and revisit it on a regular basis)], [then] they'd be well advised to set out the requirements and then really point to enabling technologies by reference perhaps but no more than that . . .

This respondent, in the quote above and throughout that portion of the interview, expressed substantial concern with the lack of technical knowledge on the part of regulators. For this respondent's organization, therefore, participation in the rulemaking process is critical to avoiding cumbersome and inefficient regulations.

[283] *See* Bamberger (2006) at 387.
[284] *Id*.

Participation in the rulemaking process is only part of the process for organizations to manage their information security regulatory exposure under HIPAA, GLBA, and FTC enforcement.[285] Compliance with the published regulations also requires extensive involvement of and reliance upon the judgment of information security professionals. Many aspects of those regulatory regimes are based on concepts of "reasonableness," whether a function of the industry, size and scope of the firm, or sensitivity of the information resources being protected. As described above in Sections 2.7.2, 2.7.3, and 2.7.4, each of HIPAA, GLBA, and FTC enforcement have management-based regulation aspects targeted at various stages of the ISPL that, rather than prescribing specific performance standards, command the regulated entity to act to protect its information assets in a manner reasonable given the factors noted above. This creates an environment of substantial uncertainty for non-technical managers seeking to maintain compliance.

As noted by Bamberger and Mulligan (2011), "[p]rofessionalism has long served as an important institution for mediating uncertainty in the face of environmental ambiguity."[286] They explain how "[i]n the privacy context, increasing ambiguity as to the future behavior of both regulators and market forces prompted a parallel escalation in the reliance on internal corporate experts, grounded in knowledge and experience of privacy regulation's trajectory, to guide corporate practices and manage privacy risk."[287]

A similar condition exists in the information security space. In addition to the regulatory environment, discussed above, creating an uncertain environment for organizations, two conditions worth noting exist that contribute to this similarity. First, privacy and information security regulation are highly interrelated in all of HIPAA, GLBA, and FTC enforcement.[288] Second, as discussed further in Section 4.1.1.2 below, information security is an exercise in risk management – specifically in mitigating uncertain and unpredictable[289] risk. In the remainder of this section, I identify results from the CISO interviews supportive of their use to reduce uncertainty in the regulatory environment.

One respondent from the healthcare industry discussed how their role in the risk management process was essential as HIPAA began to take effect. The respondent described the activities their firm engaged in at that time as follows:

[285] I notably exclude state "reasonable security" statutes from this discussion, primarily because of a dearth of enforcement of those statutes. As of the time of this writing, the author is unaware of any substantial enforcement actions resulting primarily from the state "reasonably security" statutes discussed above.

[286] Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247, 294 (Jan. 2011).

[287] *Id*.

[288] *See, e.g.*, Privacy and Security, http://business.ftc.gov/privacy-and-security (last visited Apr. 10, 2011).

[289] Consider, for example, the concept of a "zero-day" exploit – a system vulnerability discovered by an attacker, unknown to the system operator, and for which a patch or other defense mechanism has not yet been developed.

> . . . [s]o we sat down with the various fields of information we were collecting and we came up with our own definition of de-identified data and so that when HIPAA came actually, there was actually a very high degree of correlation having just sort of thought through as a practical matter, you know, where the risks lie. [As a result,] [t]here was very little change to our systems when HIPAA came along.

In this instance, the risk management role of the information security professionals within the respondent's organization apparently was successful in managing the risk – and uncertainty about the result of the regulatory process – such that when the final regulations came through, according to the respondent, very little changes were necessary to their processes and procedures to achieve compliance. Interestingly, this was the only respondent who reported having an advantage in the compliance process. One other respondent reported that they had some initial familiarity as HIPAA became effective but it was unclear to what degree they were familiar or why. Three respondents reported HIPAA as "stirring up a lot of changes."

Another respondent from the healthcare industry identified how HIPAA raised the profile of security within their organization. The respondent described how:

> . . . there was such a buildup for HIPAA, it was almost a Y2K kind of buildup . . . it [] became socialized in a way that it made security a bit more respectable.

This respondent directly identifies how HIPAA raised profile of information security professionals within their organization. Six total respondents (including the above) described conditions suggesting they experienced a similar boost in their professionalism, although only one respondent in addition to the above directly stated as much.

Another respondent from the healthcare industry directly spoke to their participation in the HIPAA rulemaking process discussed above. The respondent described how they were:

> . . . meeting with some folks at NCVHS [the National Committee on Vital Health Statistics] . . . and they're looking at the whole issue of de-identified data and re-identification risk . . . 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 one of the discussions we were having was whether or not it made sense for them 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.

This is one of the more striking quotes from the CISO interviews for several reasons. First, it clearly identifies participation in one of the rulemaking advisory groups specifically referenced in the HIPAA statute – perhaps the strongest support for Hypothesis **H9a** recorded in the interviews. Specifically, the respondent – in the context of representing their organization – played an important role in the Committee's work even though the respondent was not an actual member of the Committee.[290] Second, the respondent identifies that they were already engaged in several of the activities under consideration to become regulation. This is further evidence consistent with that discussed above that organizations subject to HIPAA relied on information security professionals to help reduce uncertainty in advance of regulations taking effect – and may be successful in doing so. Finally, it is interesting to note that the respondent views these particular changes important as a policy matter – i.e., that they see value to all organizations engaging in a similar practice. This suggests that the respondent, and perhaps the organization they represent, consider the network externalities (both positive and negative) produced by information security choices to matter. Such a finding – although beyond the scope of the questions asked in the CISO interviews – might correlate with my earlier discussion (Section 2.4.2) of how information security may be both an outcome and a process for achieving an outcome. Specifically, as discussed in that section, there may be certain desirable "practices" which, although not directly (casually) linkable to objective security outcomes like breaches, become desirable "outcomes" themselves because of their risk mitigation effect.

Another respondent from a financial services company described how their organization participated in the rulemaking process for the Payment Card Industry Data Security Standards (PCI-DSS)[291], indicating that they:

> [J]oined the PCI Security Standards Council as a member of the advisory board, precisely so that we could give input to what works and what doesn't work and ensure that the thing becomes better at dealing with the needs of the industry without throwing the baby out with the bath water.

While PCI-DSS is not formal law in most jurisdictions,[292] this example is worth noting because of the emphasis the respondent placed upon their participation in the PCI-DSS rulemaking process. This is particularly interesting given that the respondent reported this information prior to the passage of Nevada's law, which is the only jurisdiction currently to have adopted PCI-DSS in its entirety. Without digressing too much from my

[290] An interesting follow-up effort would be to determine, perhaps by survey, for how many healthcare firms subject to HIPAA regulation this is/was true at various stages of the HIPAA rulemaking process.

[291] *See* PCI SSC Data Security Standards Overview, https://www.pcisecuritystandards.org/security_standards/index.php (last visited Apr. 11, 2011).

[292] Three notable exceptions exist: 1) Minnesota, which requires partial PCI-DSS compliance (*see* MINN. STAT. § 325E.64); 2) Nevada which requires full PCI-DSS compliance, incorporating the standard by reference in the statute (*see* NEV. REV. STAT. § 603A.215); and 3) Washington State, similar to Minnesota in adopting select portions of PCI-DSS (*see* WASH. REV. CODE. § 19.255.020).

central analysis in this paper by introducing a tangential area of law,[293] it is worth highlighting this example as another instance of an organization committing substantial resources to participating in a regulatory rulemaking process.

The analysis of the law above and the empirical evidence revealed by the CISO interviews suggests support for Hypothesis **H9a**. While the interviews represent only a preliminary dataset, considered together with the analysis above they describe a condition worth confirming on a larger scale. This analysis also sets up the next section, in which I discuss how the "reasonable security" aspects of HIPAA, GLBA, and FTC enforcement promote reliance on information security professionals to inform risk mitigation decisions for meeting reasonableness standards.

4.1.1.2 Information Security Professionals Enable Risk Mitigation in an Uncertain Security Climate

Much of my discussion thus far focuses on the role of information security professionals vis-à-vis the regulatory rulemaking process. In this section, I explore the role of information security professionals in the compliance and risk mitigation processes. To help frame this discussion, I begin by contextualizing the manager-professional relationship – that relationship most affected by compliance portion of the regulatory process.

4.1.1.2.1 The Roles of Professionals and Managers in "Command Hierarchies"

For the purposes of examining the role of information security professionals in the compliance process (Hypothesis **H9b**), the aspect of professionalism on which I focus is the relationship between these technical professionals and the senior (general) managers to whom they report. I consider these relationships under the model of Fordist/Weberian "Command Hierarchies"[294] where the relationship between the manager and the professional is governed by a concept of "rational-legal authority"[295] under which senior management are presumed to have a "legal" right – as a function of their fiduciary duty within the organization – both to: 1) ensure proper compliance with applicable laws and

[293] It will be interesting to see if other jurisdictions, or perhaps even the Federal legislature, follow the trend that certain states have of adopting portions of PCI-DSS into law. As discussed in Chapter 1, Section 3.7.4.1, SBNs were passed over a period of many years (2003-present) are as of the time of this writing still do not exist in all U.S. jurisdictions.

[294] *See generally* W. Richard Scott and Gerald F. Davis, ORGANIZATIONS AND ORGANIZING (2007) at 46-50.

[295] *See id.* at 47.

regulations; and 2) to minimize costs and maximize efficiency in the process of achieving and maintaining compliance.

This approach considers the regulated organizations examined here to be "functional" or unitary" in type.[296] This is quite obviously a vast oversimplification, and most certainly does not accurately describe the organizations studied through the CISO interviews. For the purposes of this analysis, however, the "centrally coordinated specialization" aspects of functional or unitary organizations best capture the relationship between information security professionals and the senior management to which they report. As noted above, senior management bear the legal and fiduciary responsibility for the results of the compliance activities. However, they likely lack the specialized technical expertise necessary to make sound judgments as to reasonableness in compliance – a key aspect of HIPAA, GLBA, and FTC enforcement – and therefore must depend upon (but still retain control over) technical professionals. This is not dissimilar from the characteristics of professional organizations,[297] particularly when the technical complexity aspects of the "performer" (the professional) are moved into the organization.[298]

The result is a situation in which managers are presented with two choices in the compliance context: 1) defer to the judgment of their professionals, as would be the case in a modern professional organization; or 2) attempt to supervise them explicitly in a command-style hierarchical approach. This section explores the former condition, which I propose is promoted by HIPAA, GLBA, and FTC enforcement. Section 4.1.2 explores the latter condition, under the conditions imposed by regulation setting absolute (prescriptive) standards, such as SBNs.

4.1.1.2.2 HIPAA, GLBA, and FTC Enforcement Encourage Managers to Defer to Professionals in Achieving and Maintaining Compliance

As discussed above in Chapter 2, Sections 2.7.2, 2.7.3, and 2.7.4, HIPAA, GLBA, and FTC enforcement each have aspects of management-based regulation that require organizations to develop (and adhere to) information security procedures appropriate to their individual circumstances. These procedures generally must fall within the

[296] *See id*. at 131 (describing functional or unitary organizations as those "based on departmentalization around varying specialized activities contributing to overall goals, including "line" departments, involved in activities directly related to producing or distributing goods or services, and staff departments, involved in support matters such as accounting, finance, or personnel.")

[297] *See id*. at 147-49.

[298] *Id.* at 148 (describing how "as 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.")

frameworks specified by, and cover the substantive areas addressed by, the respective regulations, but the implementation details are largely left up to the regulated entities. I again turn to the CISO interviews to illuminate how these regulatory demands affect the relationship between managers and professions.

Hypothesis **H9b** posits that regulation based on "reasonable security" standards will strengthen the role of information security professionals in organizations. This is because managers will have to rely on technical professionals' judgment as to what constitutes "reasonable" given the constraints of the regulation. In the context of HIPAA, for example, the regulations specify a "flexibility of approach" under which, with respect to (nearly) all the rules with which an organization must comply, covered entities may:[299]

> (1) [ ] use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
> (2) In deciding which security measures to use, a covered entity must take into account the following factors:
>
> > (i) The size, complexity, and capabilities of the covered entity.
> > (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
> > (iii) The costs of security measures.
> > (iv) The probability and criticality of potential risks to electronic protected health information.

These general parameters provide a great deal of flexibility to organizations with respect to compliance. They also, however, introduce a great deal of uncertainty. In determining what constitutes "reasonably and appropriately implement[ing] the standards" an organization's management must turn to professionals with appropriate expertise. As noted in Sections 2.7.3 and 2.7.4 above, both GLBA and FTC enforcement both provide similar degrees of flexibility to organizations in considering how to meet their compliance obligations.

In conjunction with the FTC's reliance upon the CISSP certification, as discussed in Chapter 2, Section 3.4 above, this need for professionals has likely been a key element in the rise of the CISSP as a predominant certification for information security professionals. The ability to rely upon a certified professional's judgment as to reasonableness within a technical field is essential to management in developing appropriate compliance plans.

[299] 45 C.F.R. § 164.306(b).

The result is a situation where managers must afford information security professionals substantial discretion in those professionals' exercise of their duties. One respondent at a financial services organization described how their organization's senior management moved to an "enterprise risk management" approach to addressing information security:

> There is an enterprise risk management framework which is actually adopted at the [name of organization] level where we have something called the Enterprise Risk Management Committee, which is chaired by [name of executive], the CFO of [name of organization]. And basically, in simplistic terms, the enterprise risk management committee is trying to establish, what are the major risk factors to [name of organization] and measure them on the scale of magnitude of event if it happened, and the speed of onset of event. [The respondent CISO identified that they were a member of this executive-level committee.]

This respondent, like nearly all the respondents, identified information security primarily as a risk-management exercise. When prompted about how this risk management framework related to regulatory compliance, the respondent described how it played an integral role in regulatory mechanisms such as the Payment Card Industry-Data Security Standard (PCI-DSS)[300] – an industry self-regulatory mechanism which, like HIPAA, GLBA, and FTC enforcement, affords regulated entities substantial latitude in determining their individual procedures for compliance. The respondent contrasted this process with the effect of Sarbanes-Oxley which they described as "too prescriptive."[301] The respondent identified one of the key advantages of PCI-DSS as "it does not legislate technology."

In another example, a respondent CISO of a healthcare organization identified the implemented regulations under the HIPAA Security Rule[302] as "a good construct." The respondent noted that:

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

[300] As noted above in Section 4.1.1.1, I do not seek to distract from my analysis by introducing another area of law at this stage in the analysis. Nonetheless, the structural similarity of PCI-DSS (its regulatory delegation aspect) and this respondent's striking comments as to how that aspect affected the respondent's role vis-à-vis the organization's senior management makes reporting of this data worthwhile.

[301] In Section 4.1.2 I contrast this respondent's and others' responses regarding "prescriptive" legislation that sets absolute standards and how regulation of that form differentially affects the manager-professional relationship in regulated firms.

[302] *See* 45 C.F.R. § 164.308.

Without specific standards in these regards, managers are forced to turn to technical professionals to fill in the gaps in implementation. As discussed above in Chapter 2, Section 2.6.2.3, this may well have been intention in the context of HIPAA. The result is, as noted in this example and the others discussed in this section, a condition under which the style of regulation substantially influences the relationship between managers and professionals, strengthening the role of professionals and increasing the need of managers to rely upon professionals' discretion and judgment.

4.1.2 Regulation that Encourages Compliance with "Absolute" Standards

Regulation that lays out absolute standards, or prescriptive legislation, becomes a foil to the development of the professional within the organization. Such regulation creates a condition under which the "reasonableness" of the professional's judgment is relegated to (at best) a secondary "desirable," in favor of efforts to meet specific compliance goals. The following hypothesis results:

> **Hypothesis H10: regulation that focuses on compliance with absolute standards weakens the role of information security professionals within organizations.**

In the information security space, SBNs are the primary example of "prescriptive" laws. As discussed in Chapter 2, Section 2.7.1, every jurisdiction's statute contains an exception from reporting obligations for compromised data that was encrypted. This straightforward, absolute standard creates a condition under which "reasonableness" does *not* matter – if qualifying personal information was compromised, and it was not encrypted, the notification obligations of the statute are triggered. It becomes irrelevant whether the organization had the most "reasonable" security procedures in place, the breach holds the organization accountable for reporting the event – and therefore publicly accountable. This Section explores how SBNs, as a form of "absolute" prescriptive legislation, serve as a foil to the development of professionalism in information security by driving managers in command hierarchy relationships to override the judgment of their professionals in favor of compliance-oriented measures. The CISO interview data is particularly illustrative in this regard, as several CISOs specifically called out the way in which SBNs were changing the way in which their work was being managed "from above."

One respondent from a healthcare organization, whose notable comments appear in several other places in this paper, identified SBNs as fundamentally reversing the course their organization took with respect to information security:

> 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. [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.

Here the respondent describes an initial goal wherein management (apparently) sought the respondent's expertise to make judgments as to the most salient threats and allocate the organization's limited information security resources accordingly. The respondent suggests, however, that SBNs brought about a sea change in this regard, which they later explain:

> Then what happened, the Notification Laws came in and said, you don't need to be thinking about that because that's really not that embarrassing. You get hacked, and everyone will say, 'eh, you got hacked. Well that sort of thing happens.' Okay, what you really need to be worried about is someone losing a laptop of a backup tape falling off the track. That's what you really need to worry about because that's the stuff that not only happens a lot more frequently, it also [makes your organization look] a lot more incompetent.

Here the respondent describes a change in focus by management from attention on risk management and mitigation to avoiding public embarrassment and SBN reporting requirements. The respondent then goes on to describe how their organization moved to a mode of operation in which senior management specifically directed the respondent's information security efforts:

> 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. It's still a breach.

In this example, the prescriptive nature of the encryption exception in SBNs has created a condition where the professional judgment of the CISO in this organization is no longer sought as the primary determinant for resource allocation. Perhaps more interesting is the fact that, at least in this organization, the allocation of resources to "compliance" with SBNs appears to be occurring over the professional objection of the respondent CISO. The CISO's professional role is apparently substantially diminished by the presence of SBNs, a striking example supportive of Hypothesis **H10**.

In another example, a CISO of another healthcare organization described SBNs as extremely straightforward legislation with which to comply:

> California's [SBN] law is very strict, but it's also very clear for the most part. . . . For instance, if encrypted data are involved, then it's not a breach. . . . We feel pretty comfortable under the California [SBN] law that it makes sense to protect the unencrypted data, therefore you would expect that to drive an internal policy

> of encrypting data as much as you can, to the extent that that's feasible, so that you are protecting the data under the standard that's imposed by that particular law.

This respondent's statements clearly indicate a directive policy in their organization toward encrypting data as a function of the compliance demands of SBNs. Here, as in the example above, the role of the CISO-as-professional is not an element of the decision-making calculus – the decision to encrypt is driven entirely as a straightforward regulatory "compliance" effort. This example is also supportive of Hypothesis **H10**.

Finally, it is worth noting in the context of SBNs, that the concept of "encryption" in current statutory forms may not provide the protection regulators desire in practice.[303] Consider, for example, the Sequoia Voting System. According to a review conducted by several technical scientists, this system – while accurately claiming to implement cryptographic systems to protect the integrity of voting information, the system actually employed several poor implementation practices that rendered it substantially vulnerable to attack.[304]

This Section illustrates the example of SBNs as a foil to the development of professionalism in information security. In the next Section, I briefly consider both these factors together in the context of four conditions necessary for successful command-style hierarchies to function.

4.1.3 Evaluating the Impact of Information Security Regulation on the Effectiveness of "Command-Style" Hierarchical Relationships Between Senior Management and Information Security Professionals

This Section ties together the analysis above and elucidates conditions for when a "command-style" hierarchical approach to manager-professional relationships[305] can function. I evaluate this in the context of each of the styles of regulation discussed above, and suggest considerations for the policymaker based on this analysis.

[303] *See* supra n. 67 and n. 68.

[304] *See* Matt Blaze, et al., *Source Code Review of the Sequoia Voting System* at §§ 3.2.1 – 3.2.4 (Jul. 20, 2007) *available at* http://www.sos.ca.gov/voting-systems/oversight/ttbr/sequoia-source-public-jul26.pdf.

[305] As noted above in Section 4.1.1.2.1, I describe here the relationship between the manager and the technical professional, which does not necessarily correspond to the overall organizational structure. Most of the respondents' organizations in this study, in fact, were not from organizations that at all resembled a traditional Fordist hierarchy. The relationships between information security professionals and their senior management, however, did fit the model of a command-style hierarchy in most cases. It would be interesting as a future research topic to survey a statistically valid population of CISOs to investigate both if this relationship held true during the period of the original interviews and if it still holds true today given the rise in public attention to information security over the past few years.

There are four conditions necessary for Fordist/Weberian "command-style" management hierarchies to work effectively. First, supervisors must be able to know when their subordinates are wrong about something (Condition **C1**). Second, supervisors must know how to correct subordinates' mistakes (Condition **C2**). Third, subordinates must be fungible – there must be a market for other professionals of equal or greater ability to replace them (Condition **C3**). 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 (Condition **C4**).[306]

Applying these conditions to the two categories described above in Sections 4.1.1 and 4.1.2 yields two (perhaps obvious) results. First, regulation that encourages reliance on professional discretion is disruptive of the command-style hierarchical relationships between managers and professionals. Second, regulation that prescribes clear, "absolute" standards for compliance is well-suited to command-style hierarchical relationships between managers and professions.

Regulation that encourages reliance on professional discretion is disruptive of command-style hierarchical relationships because it necessarily creates an environment violative of Condition **C2**. As discussed at length above, 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 necessary knowledge to correct their subordinates' mistakes. In fact, because of the disjunction between security outcomes and good security practices discussed in Chapter 2, Section 2.4.2, it is unlikely that managers will even be able to identify subordinates' mistakes, thus violating Condition **C1**.

By contrast, regulation that prescribes clear, absolute standards for compliance is well-suited to command-style hierarchical relationships between managers and professionals. As discussed above, this type of regulation creates clear, measurable outcomes with which managers can identify and correct the mistakes of subordinates, satisfying Conditions **C1** and **C2**. In the case of SBNs, the clear linkage between whether or not compromised data was encrypted and whether or not an incident must be reported establishes a straightforward connection for managers to be able to link the consequences (reporting a breach incident) of a subordinate's mistake (failing to encrypt personal information covered by the statute). Thus Condition **C4** is likely to be satisfied under the environment created by this type of regulation. As to Condition **C3**, insufficient data exist as to measure the fungibility of information security professionals, however the existence of the CISSP certification and its broadening use, as described in Chapter 3,

[306] These criteria were developed with Todd LaPorte (UC Berkeley Department of Political Science) and are partially derivative from the following works: W. Richard Scott and Gerald F. Davis, ORGANIZATIONS AND ORGANIZING 124-181 (2007), James D. Thompson, ORGANIZATIONS IN ACTION 117-141 (2007).

Section 3.4, suggests that even if Condition **C3** is not currently satisfied, it would likely to become so in the near future.

When considering what form of regulation to employ, the policymaker should consider the differential effects of these two models of regulation on different organizational styles. The overwhelming characterization by the CISO respondents of information security as primarily a “risk management” exercise suggests policymakers may wish to err more on the side of regulation that promotes professionalism. However, for certain types of industry-specific regulation where the regulated entities are highly homogeneous, the regulator may wish to consider alternative approaches as these may better suit the capabilities and style of the existing organizations.

4.2 FURTHER RESEARCH

Perhaps the greatest empirical shortcoming of this Chapter is, ironically, the preliminary nature of the CISO interviews. I describe this as ironic because it is in fact the semi-structured approach of these interviews – as discussed in Chapter 3, Section 3.8 – that informed many of the hypotheses in this Chapter. Lacking substantial background research upon which to draw, the semi-structured nature of these interviews allowed exploration of topics salient to key practitioners in the field of information security. Unfortunately, at the same time, it limited both the sample size (as a practical matter) and the consistency of responses such as would be desired to empirically *test*, as opposed to *explore*, the hypothesis in this section.

In future research, it would be informative to develop a narrowed set of questions that could be posed to a larger sample population of CISOs (or their functional equivalents). These questions could be refined sufficiently to allow delivery in a survey format, enabling the possibility of statistically-valid sample population sizes. In my future research I intend to explore these possibilities.

An additional avenue for future research that would be interesting (if not necessarily feasible) involves interviewing attorneys who work in this area. Undoubtedly, leading data privacy and security practitioners who represent the organizations studied herein would have valuable insight into the challenges faced by those organizations and how regulatory structures affect the organizations. As an academic, I would be eager to investigate this potentially rich source of information, however as a practitioner myself, I suspect that the privilege issues involved would present an insurmountable hurdle to conducting research of this nature. Nonetheless, I do identify it in the hopes that others with far greater professional practice experience will consider whether appropriate structures to allow such research can be developed.

4.3 Conclusions

As discussed in the introduction, this Chapter seeks to utilize the framework developed in Chapter 2 to evaluate the role differing styles of regulation may have impacting the relationships between senior managers and information security professionals in large U.S.-based organizations.

The relationships between senior managers and information security professionals, as indicated above, further research is clearly indicated before any solid conclusions can be drawn. My analysis here serves both to lay the groundwork for what methods that future research might utilize, and what hypotheses could be tested. My intuition from the CISO interviews, my extensive analysis of the law, and my own professional experience is that there are profound implications for professionalism consistent with the hypotheses outlined above.

5 Conclusions and Further Thoughts

This dissertation began with a desire to understand the character and function of the legal structures regulating information security in the United States. It examined 1) how can we classify information security laws to understand their function; 2) what types of effects did information security laws have on organizations' security practices; and 3) what implications do the function of these laws have for the structure of and professional relationships within organizations. While preliminary in many regards, it is my hope that this research has suggested avenues for future scholars to more deeply investigate these questions.

As discussed in the Introduction to this Dissertation, current information security regulation in the United States is focused on protecting specific information considered sensitive to consumers rather than protecting the overall "health" and "security" of information and control networks. The conclusions in this research, however, are applicable beyond the scope of consumer protection. First, as discussed in Section 3.11, some of the evidence suggests the conclusion that the more "general" security goals outlined in management-based regulatory delegation models are effective at improving organizations' capacity to later address specific security goals such as the prevention of data breaches involving personal information. If this condition is applicable to other specific goals, as I suspect it is, that result would suggest the efficacy of management-based regulatory delegation models in addressing issues involving the overall security of control networks, such as electric "Smart Grids." Second, the security measures discussed in many of the consumer protection models are not substantially different than those described in the professional certification (CISSP) literature. Consider, for example, the security "goals" required of organizations implementing information security plans under HIPAA (Section 2.7.2), GLBA (Section 2.7.3), and the FTC's enforcement actions (Section 2.7.4) and compare them with the CISSP Domains discussed in Section 3.4. The substantial overlap present further suggests the applicability of this research to informing information security regulation aimed at goals other than protection of sensitive consumer information.

There are two additional results to which I wish to draw the reader’s attention. First, the two conclusions in Chapter 3 regarding the comparative effect of management-based regulatory delegation models and Security Breach Notification laws on organizations’ capacity to prevent breaches of personal information. As discussed in the Conclusions to that Chapter, current data suggest these models together work more effectively at preventing breaches than does either model alone. This finding has important implications for policymakers. Second, the typology I propose in Chapter 2 for classifying information security laws is of particular import for future research. Any effort to compare and contrast the effect of different regulatory structures should begin with a common basis for evaluation, and it is my hope that this typology will allow the “innovative” nature of existing and forthcoming information security laws to be evaluated with sufficient granularity in a single framework.

6 APPENDICES

6.1 *APPENDIX A – METHODOLOGY FOR SELECTING* T_1 *AND* T_2

This appendix provides a complete description of the methodology used to select points t_1 and t_2, which correspond (respectively) to the points in time when Security Breach Notification laws began to take effect and when their effect reached saturation.

(For the purposes of making this Appendix more digestible to the reader, the introductory (3.7.4.1) and concluding (3.7.4.2) sections from Chapter 2.8, Section 3.7.4 – Determining the Appropriate Time Period for Analysis are included in this Appendix as Sections 6.1.1 and 6.1.1.4 below.

6.1.1 Determining the Appropriate Time Period for Analysis

Perhaps the most challenging part of my analysis was determining over what time period(s) to perform analyses, particularly linear regressions describing the rates of change of breach incidence (for use in evaluating the results of **Method 1** and of **Method 2**). The DataLossDB database includes incidents dating back to August 1903, however coverage before the year 2000 is spotty with most years not even having a single incident. The year 2000 is the first year for which there are incidents fitting my criteria in that year and every subsequent year.[307] Part of the difficulty with this database is that, prior to the introduction of SBNs, firms had little incentive to report breaches on an individual basis. While some limited reporting was suggested under regulations promulgated pursuant to the Gramm-Leach-Bliley Act (GLBA),[308] reporting was not mandatory and did not serve to raise reporting standards to a level sufficient to provide insight into either of Hypothesis **H5** or **H6**. Thus there is not a meaningful baseline from which to establish breach incidence rates prior to the introduction of SBNs, and therefore with which to correlate whether breach incidence increased with increased use of the Internet and other interconnected information systems. For these reasons, I selected to work with data from January 2000 (t_0) onward.

[307] There are incidents meeting my criteria in 1998, however there was only one in 1999. While I did want to have some data from before the introduction of the first SBN statute, I determined that adding these additional two years of data would unduly bias the higher-order polynomial regressions over the entire dataset as they would introduce too many months with zero incidents.

[308] *See* Determination and Notification of Failure to Meet Safety and Soundness Standards and Request for Compliance Plan, 66 Fed. Reg. 8640 (amending Appendix B § III(c)(1)(g) to 12 C.F.R. Part 570)).

6.1.1.1 When SBNs "Take Effect" – Selecting t_1 and t_2

In selecting periods of analysis for Hypotheses **H5** and **H6**, I need to identify two points t_1 (when SBNs started to affect firms) and t_2 (when SBNs affect reached saturation and all firms generally were affected). Using the DataLossDB data,[309] however, it is impossible to determine "when" a company became subject to SBNs as they are state laws and were enacted over a period of several years. Unlike with most law 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. 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.[310] Thus information about which states' laws would be triggered is completely endogenous to each incident listed in the database.[311] Therefore unlike with traditional state-by-state analysis where one looks to the domicile of a firm to determine if it is affected by regulation it is impossible for the outside observer to make such a determination.

The result is a situation in which measuring what happens "after the introduction of SBNs" is difficult. The most challenging part of comparing the rates of change described above, therefore, is determining an appropriate t_1 to use as the point after which SBNs "affect" organizations. Since, as described above, it is impossible directly to establish this point, I propose the following approaches (**Method 3** and **Method 4**) to infer the appropriate period over which to analyze breach incidence for the t_1 and t_2 inflection points.

[309] Nor have I been able to identify any other (unclassified and unprivileged) data sources that could address this question. One possible data source might be billing information from law firms providing counsel on data breach incidents, however this information is protected by attorney-client privilege laws. Furthermore, to reach statistical significance, a substantial amount of this billing information – from many firms – would be required, making it unlikely that a sufficient number of law firms would be able each to convince a sufficient number of clients to allow that information to be released – even in aggregate, anonymized form – so as to render this a workable approach.

[310] 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).

[311] 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.

6.1.1.2 Differential Running Averages (Method 3)

The first approach attempts to determine the point at which the difference between the averages of all months before SBNs became effective (pre-t_1) and all months after SBNs became effective (post-t_1) is greatest. It uses a running averages model, calculating the average before and after each hypothetical t_1 for each of PREs and PUEs. For each candidate t_1, it then takes the sum of the averages for PREs and PUEs before t_1 and compares that to the sum of the averages for PREs and PUEs after t_1. The candidate t_1 with the greatest difference between these two sums is selected. The theory behind this approach is to select the point for t_1 that maximizes the impact of SBNs on increased reporting rates.

This approach has two potential applications for Hypotheses **H5** and **H6**. First (**Method 3a**), it can provide a possible t_1 for use in both **Method 1** and **Method 2**. Second (**Method 3b**), as discussed later in this section, it can be used to calculate the relative rates of change in breach incidence after t_1 with respect to the initial rise in reporting for use in **Method 2** only.

*6.1.1.2.1 Selecting a t_1 (**Method 3a**)*

Starting from the assumption that SBNs will necessarily result in an increase in reporting, and using the results of the monthly grouping described above (and displayed in *Figure 1* below), t_1 is selected by maximizing the difference between the mean of all points before a given t_1 and all points thereafter. To accomplish this calculation, I wrote a simple analysis program[312] that iterates through all candidate t_1's and computes the average of all months' breach reporting rates before that month for PREs (M_A), the average of all months' breach reporting rates before that month for PUEs (M_C), the average of all months' breach reporting rates after (and including) that month for PREs (M_B), and the average of all months' breach reporting rates after (and including) that month for PUEs (M_D).

[312] *See* Appendix C.3.

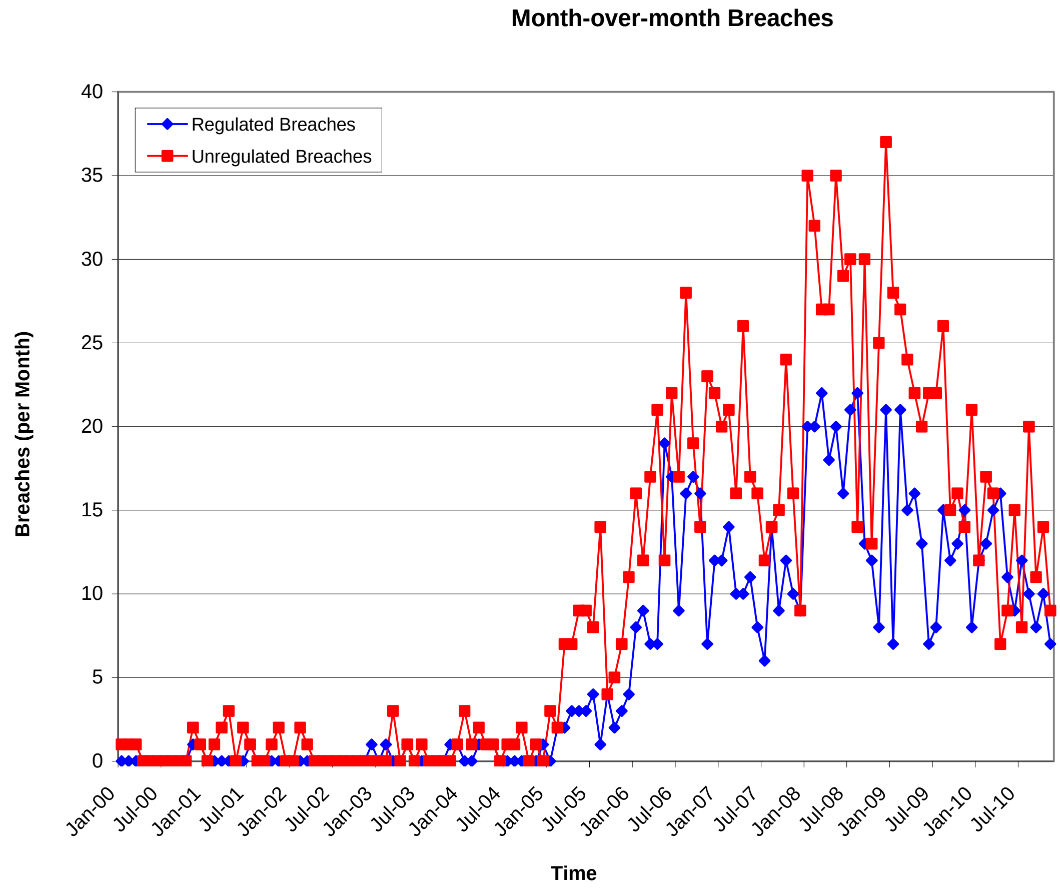


Figure 1 – Monthly Breaches for PREs vs. PUEs

A visual inspection of *Figure 1* reveals that the appropriate selection for t_1 will be approximately January 2005. My analysis program discussed above revealed that the greatest difference between the pre-t_1 and post-t_1 monthly breach averages occurs with a t_1 of December 2005. With a t_1 of December 1, 2005, the monthly average of breach incidence before t_1 is 0.597 per month (M_A) for PREs and 1.750 per month (M_C) for PUEs. The monthly average of breach incidence after t_1 is 12.783 per month (M_B) for PREs and 19.517 per month (M_D) for PUEs. The difference in mean breaches per month (before and after $t_{1)}$ is 12.186 for regulated firms and is 17.767 for unregulated firms.

*6.1.1.2.2 Calculating Differential Rise in Breach Incidence (**Method 3b**)*

Having selected this t_1, the relative rates of change described in the problem above can be determined by comparing the mean (over time) of all breach incidents before and after t_1 both for PREs (before = M_A, after = M_B) and for PUEs (before = M_C, after = M_D). This is accomplished by taking the slope of the line between M_A and M_B (S_R) and comparing it to the slope of the line between M_C and M_D (S_U). S_R and S_U are calculated as follows. First, by taking the point halfway between January 1, 2000 and t_1 (x_a = 36 (corresponding to 36 months from 01/01/2000, or 12/1/2002)) and matching it to each of M_A and M_C. Second, by taking the point halfway between t_1 and 12/31/2010 (the end of the dataset) (x_b = 102 (corresponding to 102 months from 01/01/2000, or 06/01/2008)) and matching it to each of M_B and M_D. This yields two Cartesian points (x_a, M_A) and (x_b, M_C) representing the line modeling increase in reporting for PREs and two Cartesian points (x_a, M_B) and (x_b, M_D) representing the line modeling increase in reporting for PUEs. The slope of the line between (x_a, M_A) and (x_b, M_B) is S_R and the slope of the line between (x_a, M_C) and (x_b, M_D) is S_U. Using this formula, S_R = 0.185 and S_U = 0.269. Given these values, the relative increase in breach incidence per month for unregulated firms is 1.454 times that for regulated firms.

The relative difference between S_R and S_U suggests that after SBNs "became effective" (t_1) and overall reporting increased, PREs experienced a smaller increase in reporting than PUEs. This difference may be attributable, consistent with Hypothesis **H6**, to the fact that PREs had employed greater security measures than PUEs prior to the introduction of SBNs. While these results do not directly link the adoption of security practices to the prior regulation (HIPAA/GLBA) to which PREs were subject, the correlation is consistent with this hypothesis subject to the limitations of this method discussed below.

6.1.1.2.3 Limitations

These elements of **Method 3** are heavily dependent on the absolute rise in reported breach incidence after the introduction of SBNs. As such, the differences between PREs and PUEs may be affected by factors other than regulation such as: 1) the attractiveness as targets of the organizations in those groups; 2) the number of organizations within those sectors; and 3) the degree to which organizations in those sectors have non-regulatory incentives to protect their systems. Considering the limitations of the data available (discussed above in Section 3.7.4) in the DataLossDB database, **Method 3** does not readily present a solution to control for such variations. As such, I do not endorse use of its selected t_1 for later analysis and suggest its value only as possibly providing further validation for the other methods discussed in this paper.

6.1.1.3 Polynomial Regression of the Analysis Period (Method 4)

An alternate approach (**Method 4**) to determining the inflection points t_1 and t_2 discussed above in Section 3.7.2 is to regress the entire dataset, from January 2000 (t_0) through December 2010 (t_F). Doing requires the use of polynomial regression, likely with polynomial curves of orders 3 or higher. I originally had intended to use this approach solely to validate the linear regressions proposed in Section 3.7.5, however based on the results of the Differential Running Averages approach and feedback from colleagues,[313] employing this second approach seems a prudent measure.

Method 4 proposes running polynomial regressions on the entire dataset from t_0 through t_F. Visual inspection of the dataset over this period (see *Figure 1*) suggests that at least a third-order polynomial will be required to fit the data after roughly after t_1, and accounting for the entire data series (including the negligible reporting prior to t_1) may require even higher order polynomials. As will be discussed later in this section, my results revealed that polynomial equations above order 5 best approximated my data set. Specifically, a polynomial equation of order 6 appears to yield the (statistically) strongest fit for PREs and a polynomial equation of order 9 appears to yield the (statistically) strongest fit for PUEs.

I performed regressions over the entire dataset from t_0 to t_F. Again, the data points are grouped monthly, separating PREs and PUEs into two separate groups, resulting in total numbers of breaches being reported per-month as visualized in *Figure 1*. Using the statistical package R,[314] I performed polynomial regressions of the number of breach incidents per month over the time period t_0 through t_F for each of the PRE group and the PUE group. To simply handling of the calculations, I measured time in number of months from January 1, 2000. As each data point stores the total number of incidents for a given calendar month, I assigned the value 1 to January 2000 (representing the total number of incidents from January 1, 2000 through January 31, 2000 or one month's worth of incidents). Subsequent months were assigned integer values in increasing ordinal value for a total of 132 months or data points.

To test for the statistically-best polynomial, I ran regressions using polynomials beginning with a simple quadratic regression (order = 2) through a regression using a polynomial of order 10. R provides functionality to develop appropriate polynomials for use in this type of best fit analysis, and performs least squares analysis to determine the coefficients for each term of the polynomial that best fit the data. Using this functionality, I performed regressions for each of the set of monthly data for PREs and the set of monthly data for PUEs. The R code I used to perform these regressions is provided in **Appendix C.1**. The results of these regressions are displayed in *Figures 2a* and *2b* below and in *Tables 1a* and *1b*. Based on these results, it appears that a polynomial regression of order 5 best approximates the data for PREs and a polynomial

[313] Special thanks to Gerard Stegmaier (who reviewed a preliminary version of this paper for the Privacy Law Scholars Conference 2010) and the members of the conference who attended my presentation and provided valuable feedback. Also special thanks to Professor Ashok Agrawala of the University of Maryland Department of Computer Science, who assisted me in developing a model to work with higher-order polynomial regression.

[314] *See* http://www.r-project.org/ (calculating performed using R version 2.8.1 (2008-12-22)).

regression of order 5 best approximates the data for PUEs. These selections are based on maximizing the adjusted R-squared value[315] which measures the "goodness-of-fit" of the regression curve to the data, accounting for the increasing number of predictors added with each additional order of the polynomial used to approximate the data.[316] I then check these values against the number of coefficients exhibiting statistical significance at least at the 0.05 level for raw polynomials.[317] While the greatest R-squared values are order 6 for PREs and order 9 for PUEs, each of these exhibit a comparatively small number of coefficients with statistical significance (at any level). The order 5 (raw) polynomials for each of PREs and PUEs have only slightly smaller R-squared values and exhibit statistical significance at the 0.05 level or better for *all* of their coefficients. For these reasons, I have selected the order 5 polynomials for each of PUEs and PREs. The adjusted R-squared values and number of coefficients with significance at the 0.05 level or better for each of the regressions are provided below in *Tables 1a* and *1b*. Complete raw data is provided in **Appendix B.1** (for PREs) and **Appendix B.2** (for PUEs).

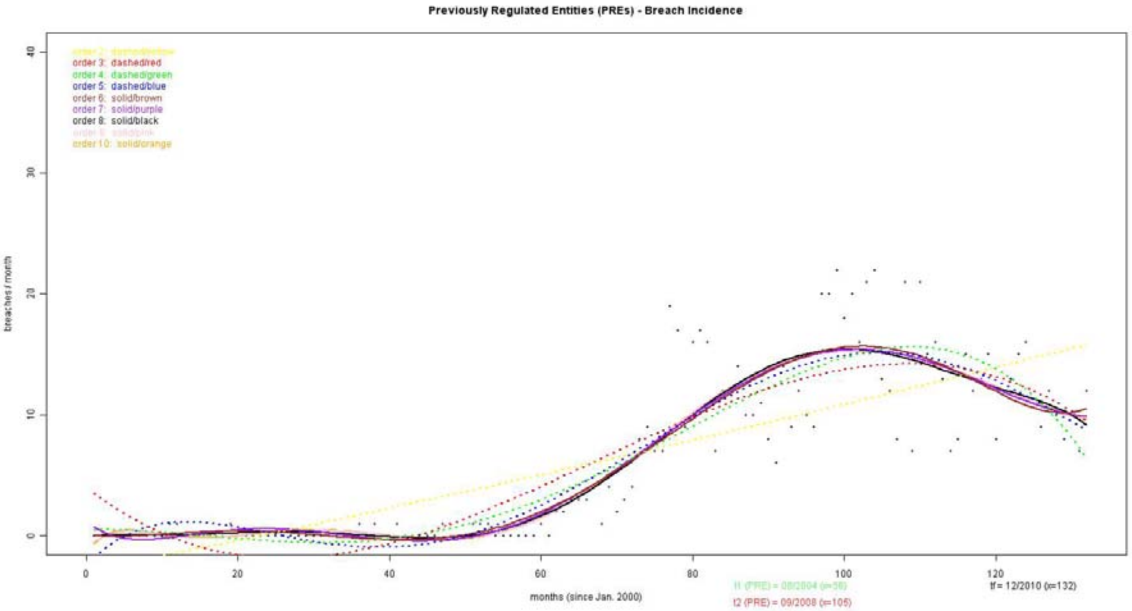


Figure 2a – Polynomial Regressions of Breach Incidence for PREs[318]

[315] Also known as the "coefficient of determination", *see* JAY L. DEVORE, PROBABILITY AND STATISTICS FOR ENGINEERING AND THE SCIENCES 504-07 (5th ed. 2000).

[316] *See* Goodness-of-Fit Statistics, http://web.maths.unsw.edu.au/~adelle/Garvan/Assays/GoodnessOfFit.html (last visited Mar. 29, 2011).

[317] *See* infra n. 321.

[318] A larger version of this chart is included in **Appendix A.1**. Note that the rendering function in R "cheats" when drawing regression curves, and uses the best-fit curve accounting for a best-case assumption about the error terms for each polynomial term's coefficient. Plotting these curves strictly according to the coefficients for each polynomial term and the intercept results in a curve that slightly deviates from these renderings, with that deviation increasing both as x increases and as the order of the polynomial increases.

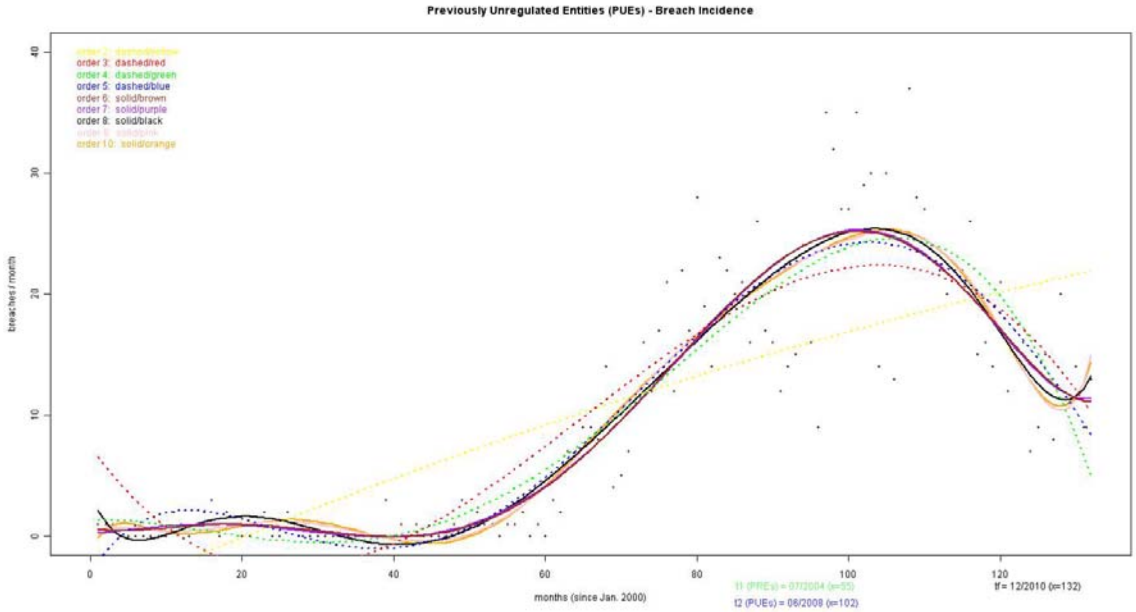


Figure 2b – Polynomial Regressions of Breach Incidence for PUEs[319]

[319] A larger version of this chart is included in **Appendix A.2**. Note that the rendering function in R "cheats" when drawing regression curves, and uses the best-fit curve accounting for a best-case assumption about the error terms for each polynomial term's coefficient. Plotting these curves strictly according to the coefficients for each polynomial term and the intercept results in a curve that slightly deviates from these renderings, with that deviation increasing both as x increases and as the order of the polynomial increases.

Order of Polynomial	Adjusted R-Squared Statistic	Number of Coefficients[320] with Statistical Significance at 0.05 or Better (by Polynomial Type)	
		Orthogonal[321]	Raw
2	0.6239	1	1
3	0.7588	2	3
4	0.7833	3	2
5	**0.7949**	**4**	**5**
6	0.8012	5	2
7	0.8007	5	0
8	0.8003	5	0
9	0.7995	5	0
10	0.7978	5	0

Table 1a – Adjusted R-Squared Values and Coefficient Significance Codes for PRE Polynomial Regressions

Order of Polynomial	Adjusted R-Squared Statistic	Number of Coefficients[322] with Statistical Significance at 0.05 or Better (by Polynomial Type)	
		Orthogonal[323]	Raw
2	0.5776	1	1
3	0.7780	2	3
4	0.8109	3	2
5	**0.8221**	**4**	**5**
6	0.8282	5	2
7	0.8270	5	0
8	0.8290	5	0
9	0.8306	5	0
10	0.8295	5	0

Table 1b – Adjusted R-Squared Values and Coefficient Significance Codes for PUE Polynomial Regressions

[320] Excluding the intercept value.

[321] Using orthogonal polynomials, R generates the same coefficients for each order of magnitude. None of the coefficients with order 7 or greater exhibited any statistical significance. Each coefficient's significance value does vary across each order of polynomial, however these significance values tend to vary only slightly. Complete tables are provided in **Appendix B.1** (PREs) and **Appendix B.2** (PUEs).

[322] *See* supra n. 320.

[323] *See* supra n. 321.

Having selected these two polynomial regressions, I examine them to determine if they exhibit inflection points consistent with the behaviors for t_1 and t_2 identified in Section 3.7.3.3 above. Lacking any external mathematical guidance to inform this selection,[324] I will examine the regression curves to determine t_1 as the first month where the curve both: 1) above its previous local maximum; and 2) is thereafter increasing until its (overall) maximum.[325] I determine t_2 in a somewhat more straightforward manner, by simply finding the overall maximum of the curve.[326] The overall maximum over the curve naturally would correspond to the point at which SBNs reach saturation effect, for (as discussed above in Section 3.7.3.3) the expected value of monthly breach incidence (and therefore the curve approximating these values) should drop thereafter.[327] Each of these regression curves (and their corresponding data points) are displayed in *Figures 3a* and *3b* for PREs and PUEs, respectively:

[324] As mentioned in Section 3.7.3.4, the lack of certain data characterizing security breach incidents requires the use of a "bootstrapping-like" approach to determining t_1 and t_2. As such, the data provides little guidance as to the selection of a methodological approach for evaluating the regression curves in selecting these two points.

[325] This is accomplished using a simple java program which iterates through the candidate t_1's and selects the appropriate one matching this condition. Since I have organized the data into monthly counts, I iterate ordinally through the integers rather than using first-order differential calculus to determine the actual inflection values.

[326] See supra n. 325.

[327] It is possible that some outlier event, such as the successful deployment of a worldwide botnet exploiting a widespread zero-day vulnerability, could result in a temporary spike in reporting sufficient to disrupt the curve into a second local – or even replacement overall – maximum. However, this does not appear to have been the case during the analysis period.

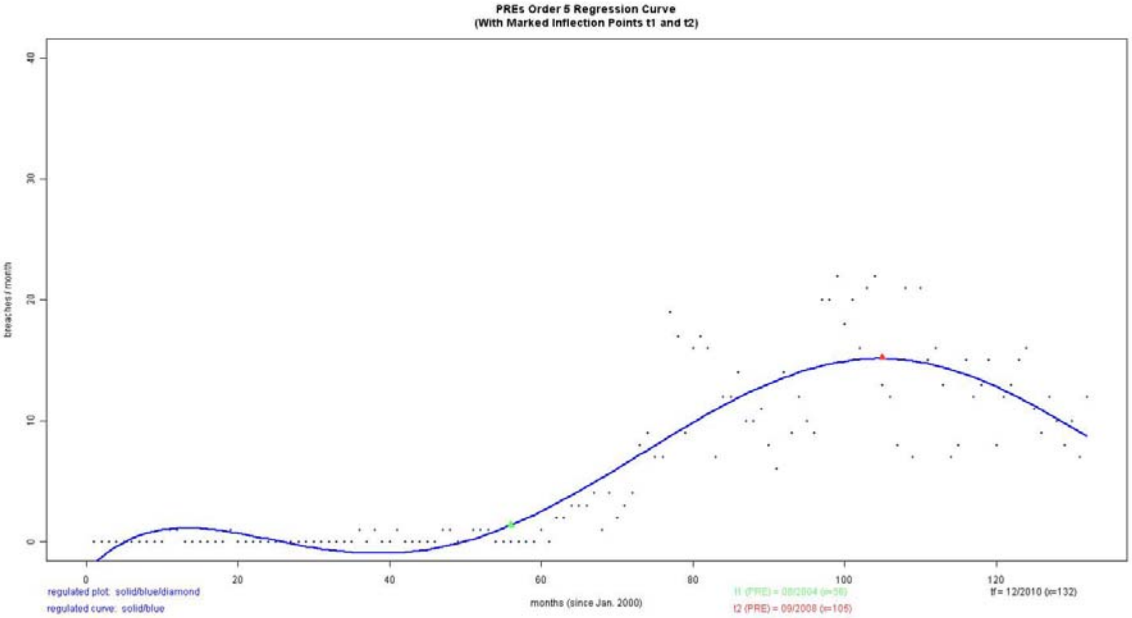


Figure 3a – Polynomial Regression Curve of Order 5 for PRE Breach Incidence[328]

[328] A larger version of this chart is included in **Appendix A.3**. Note that the rendering function in R "cheats" when drawing regression curves, and uses the best-fit curve accounting for a best-case assumption about the error terms for each polynomial term's coefficient. Plotting these curves strictly according to the coefficients for each polynomial term and the intercept results in a curve that slightly deviates from these renderings, with that deviation increasing both as x increases and as the order of the polynomial increases. For the order 5 curve, this deviation is not significant for the purposes of visualization.

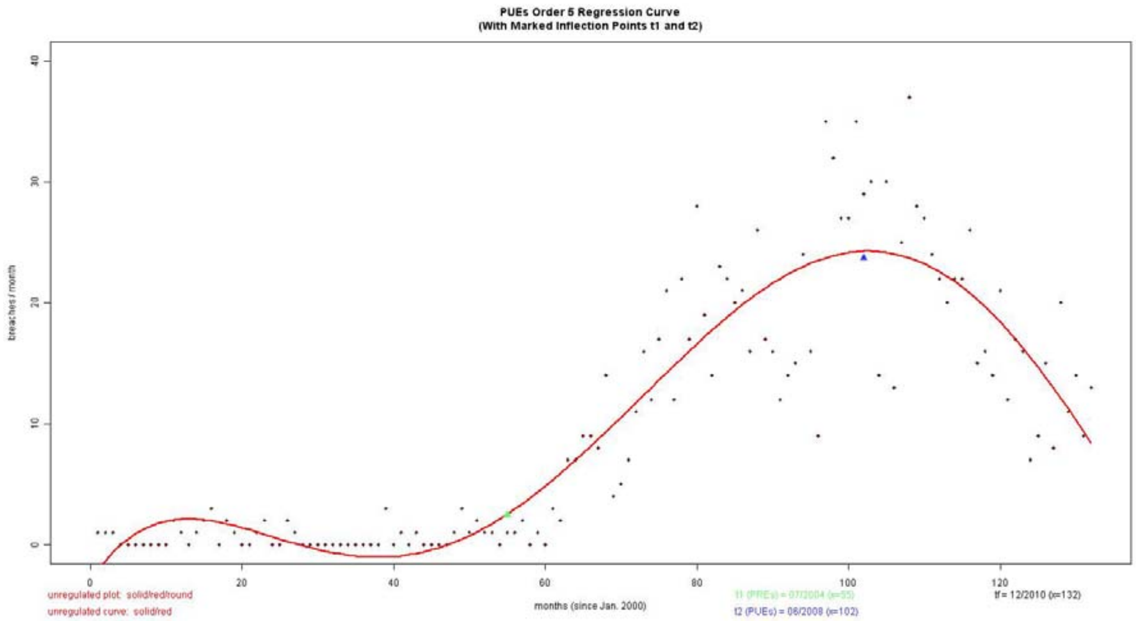


Figure 3b – Polynomial Regression Curve of Order 5 for PUE Breach Incidence[329]

The result of the analysis described above suggests a t_1 of 56 (corresponding to August 2004[330]) both for the regression curve approximating PRE breach incidence and a t_1 of 55 (corresponding to July 2004[331]) for the regression curve approximating PUE breach incidence. With respect to t_2, the PRE curve suggests a t_2 of 105[332] (corresponding to September 2008[333]) and the PUE curve suggests a t_2 of 102 (corresponding to June 2008[334]). It is worth noting that there appears to be a minor variance in R's prediction function for graphing polynomial regressions. On *Figure 3b*, the plot point (blue triangle) for t_2 (PUEs) is slightly below the actual curve. I derived this point by actually calculating the value of the function described by the order 5 coefficients and intercept

[329] A larger version of this chart is included in **Appendix A.4**. Note that the rendering function in R "cheats" when drawing regression curves, and uses the best-fit curve accounting for a best-case assumption about the error terms for each polynomial term's coefficient. Plotting these curves strictly according to the coefficients for each polynomial term and the intercept results in a curve that slightly deviates from these renderings, with that deviation increasing both as x increases and as the order of the polynomial increases. For the order 5 curve, this deviation is not significant for the purposes of visualization.

[330] Because of the way data is grouped for analysis, as noted above, a calendar date of a given month *includes* breach incidents that occurred during that month. The precise cutoff would therefore be the end of the last day of that month.

[331] *See* supra n. 330.

[332] The actual maximum on the curve appears to be at 102.5, which I round up to 103. Ordinal integer values are necessary since each integer represents a single month and data are grouped together in months for the purposes of analysis.

[333] *See* supra n. 330.

[334] *See* supra n. 330.

(see *Table 2* below) and plotting that explicitly using R's point plot function. This is likely because R's prediction function for plotting polynomial regressions attempts to account for the degree of statistical significance of each coefficient, and thus introduces a slight variance from my explicit plot (which naturally treats each coefficient as having perfect significance). However, as of the time of this writing I have been unable to locate any documentation to confirm this. In any event, this minor differential does not appear to alter the significance of my results as they pertain to Hypotheses **H5** or **H6**.

6.1.1.3.1 Additional Statistical Information/Notes

The following information briefly summarizes the statistical information reported by R pertaining to the two regression curves discussed above. Full details off all curves are reported in **Appendix B.1** (PREs) and **Appendix B.2** (PUEs).

Statistical Data	PRE Regression Curve (Order 5)		PUE Regression Curve (Order 5)	
Residual Std. Error	3.056 (on 125 DF)		4.2567 (on 122 DF)	
Adj. R-Squared	0.8012		0.8306	
p-value	< 2.2 e-16		< 2.2 e-16	
	Orthogonal Polynomials	Raw Polynomials	Orthogonal Polynomials	Raw Polynomials
Intercept [sig.]	6.1364 [***]	-2.405 [ ]	9.8258 [***]	-2.969 [ ]
Coefficient x [sig.]	62.2159 [***]	$6.398 * 10^{-1}$ [*]	90.1556 [***]	$9.419 * 10^{-1}$ [*]
Coefficient x^2 [sig.]	1.8952 [ ]	$-3.748 * 10^{-2}$ [**]	-7.4220 [.]	$-5.628 * 10^{-2}$ [**]
Coefficient x^3[sig.]	-28.7868 [***]	$7.787 * 10^{-4}$ [***]	-52.8087 [***]	$1.180 * 10^{-3}$ [***]
Coefficient x^4 [sig.]	-12.5576 [***]	$-6.118 * 10^{-6}$ [**]	-21.6911 [***]	$-9.231 * 10^{-6}$ [***]
Coefficient x^5 [sig.]	8.8689 [**]	$1.613 * 10^{-8}$ [**]	13.1077 [**]	$2.383 * 10^{-8}$ [**]
Significance Codes: [***] (0.001) [**] (0.01) [*] (0.05) [.] (0.1) [blank] (1)				

Table 2 – Summary of Key Statistical Information

6.1.1.4 **Conclusions Regarding the Appropriate Time Period for Analysis**

The analysis discussed above in Section 6.1.1.3 suggest clear inflection points in the trend of monthly security breach incidence to use as values for t_1 and t_2. The fact that the candidate t_1 is similar both for PREs and for PUEs is quite interesting, and suggests support for its accuracy. Furthermore, a visual inspection of the other candidate regression curves – both for PREs (*Figure 2a*) and for PUEs (*Figure 2b*) – suggest that the candidate t_1 would be quite similar using polynomial regressions of different orders.[335] Considering these factors, and the limitations of **Method 3** identified in Section 6.1.1.2.3, adopting the suggested candidate t_1 of 56 (corresponding to August 2004) for PREs and the candidate t_1 of 55 (corresponding to July 2004) for PUEs seems preferable to that produced by **Method 3**. Based on this analysis, therefore, it seems reasonable to suggest that an operational estimate of when SBNs began to take effect throughout the United States is between July and August of 2004.

With regard to t_2, the regression analysis above suggests a slightly broader difference between the candidates for each of PREs and PUEs. Specifically, the (order 5) polynomial regression curve for PREs has a maximum at 105 (corresponding to September 2008), whereas the (order 5) polynomial regression curve for PUEs has a maximum at 102 (corresponding to June 2008). This data suggests a candidate t_2 for PREs at 105, and a candidate t_2 for PUEs at 102. While these two candidate t_2's differ more than do the candidate t_1's, the difference still seems appropriate for the purpose of further analysis. Based on this analysis, it seems reasonable to suggest that an operational estimate of when SBNs reached saturation of compliance was in September 2008 for PREs, and June 2008 for PUEs.

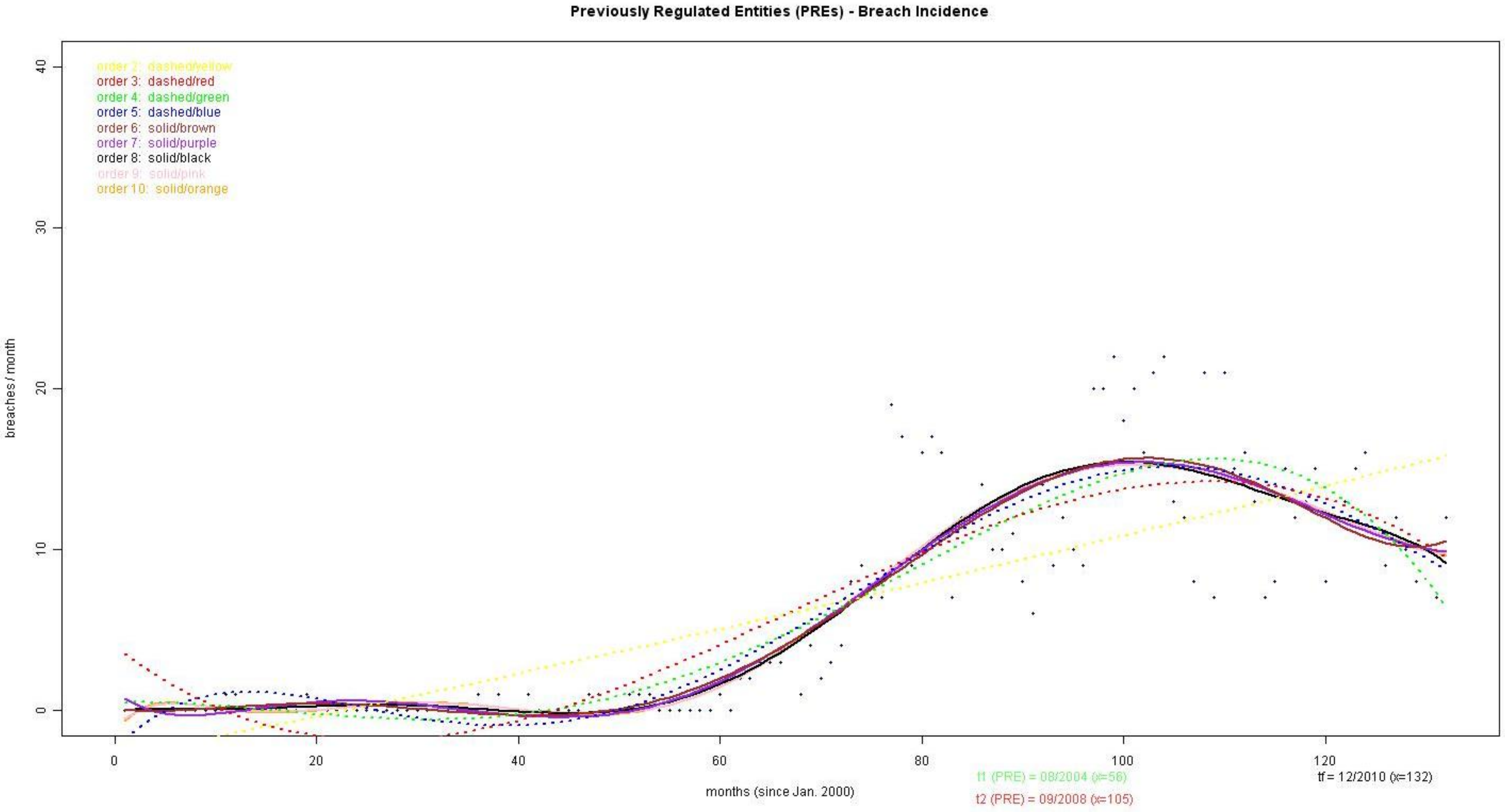
As discussed earlier in Section 3.7.3.2, the efficacy of **Method 2** would depend substantially on whether t_1 and/or t_2 varied substantially between PREs and PUEs. The analysis above suggests that t_1 varies only trivially between these groups. While that analysis does suggest some variance for t_2, the variance appears too small to suggest the efficacy of **Method 2**. As discussed earlier, for **Method 2** to be effective, it must be possible to isolate the relative rate of change in incidents (over t_1 to t_2) between the two groups from the absolute rise in incidents over this period. The only method available to accomplish this separation, given the limitations of the data, is if the periods from t_1 to t_2 vary substantially between PREs and PUEs. Such a condition might allow inferences to be drawn from the rates-of-change in breach incidence across the two groups (over t_1 to t_2) if those rates differed substantially. However, I do not believe that three months provides sufficient difference to allow for such an approach, therefore I will not endorse **Method 2** as providing insight into either of Hypothesis **H5** or **H6**. Nonetheless, I will run analysis on the period from t_1 to t_2 and report those results to potentially support future research.

Finally, with respect to differences in t_2 between PREs and PUEs, it is worth noting that a sufficiently large difference might in itself suggest something about the differences between PREs and PUEs. Specifically, if the candidate t_2 for PUEs were sufficiently later than that for PREs, it might suggest that PREs had some advantage – as a function

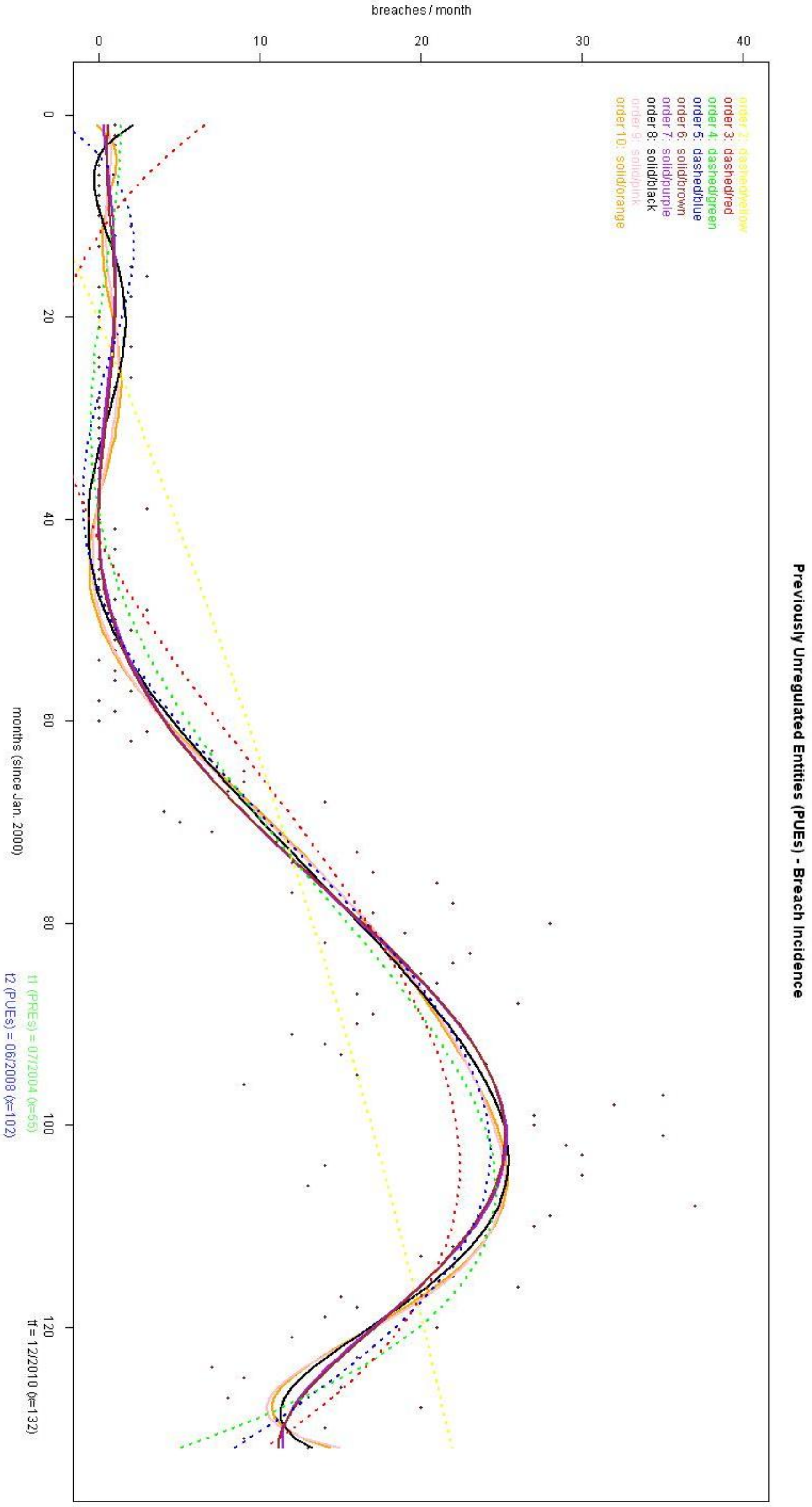
[335] Assuming that a polynomial of sufficiently high order to handle the entire time series (order > 4) is used, and discounting outliers with unusually high approximations of early negligible activity (e.g., order 5 curves both for PREs and PUEs).

of their early regulatory requirements – in complying with the requirements of SBNs. However, as was the case with my analysis above of the efficacy of **Method 2**, I do not believe a two month difference is sufficient to indicate support for such a hypothesis.

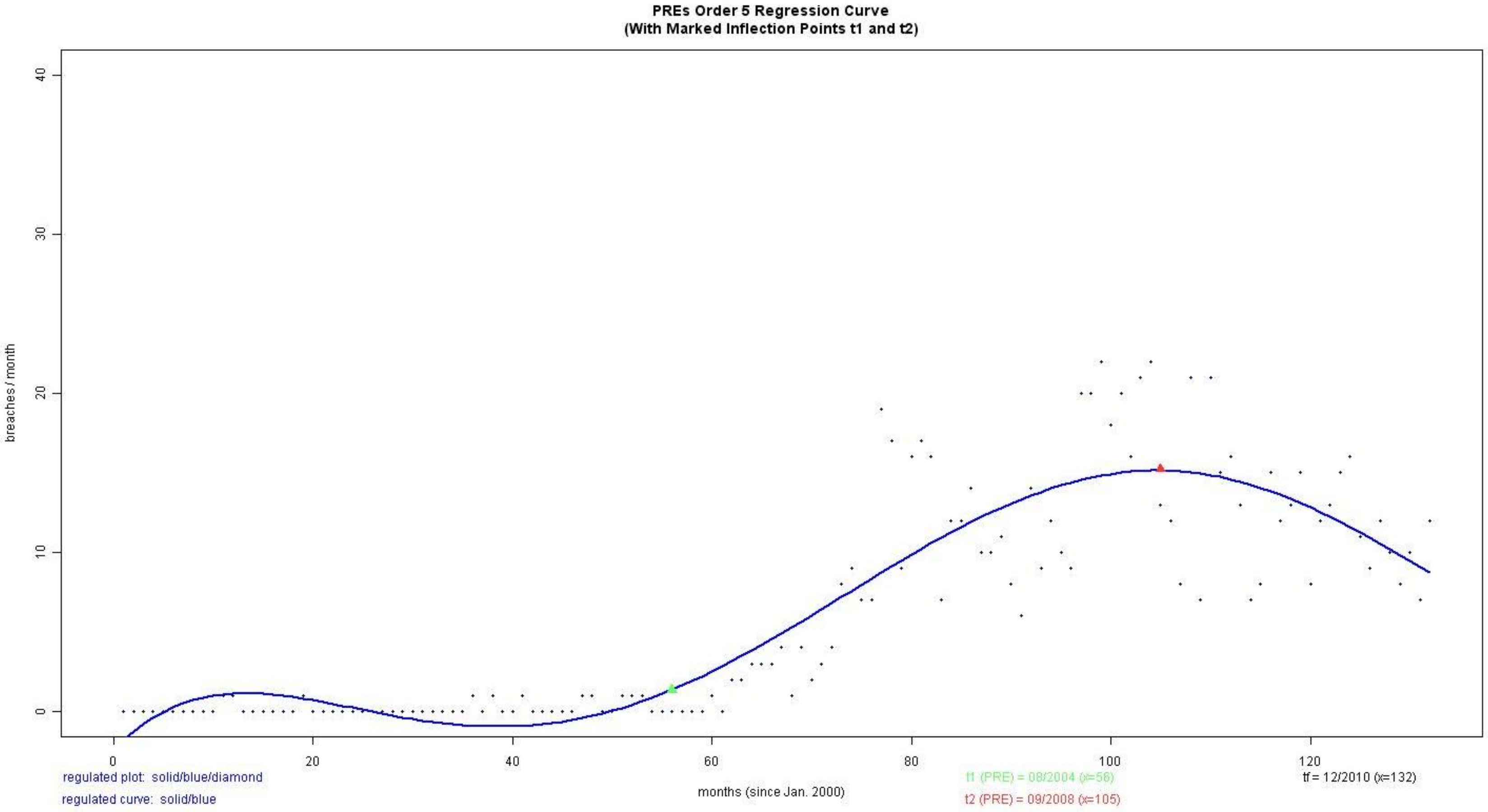
6.2 Appendix A.1 – Polynomial Regressions of Breach Incidence in Previously Regulated Entities (PREs)


Previously Regulated Entities (PREs) - Breach Incidence
order 2: dashed/yellow
order 3: dashed/red
order 4: dashed/green
order 5: dashed/blue
order 6: solid/brown
order 7: solid/purple
order 8: solid/black
order 9: solid/pink
order 10: solid/orange
breaches / month
0
10
20
30
40
0
20
40
60
80
100
120
months (since Jan. 2000)
t1 (PRE) = 08/2004 (x=56)
t2 (PRE) = 09/2008 (x=105)
tf = 12/2010 (x=132)

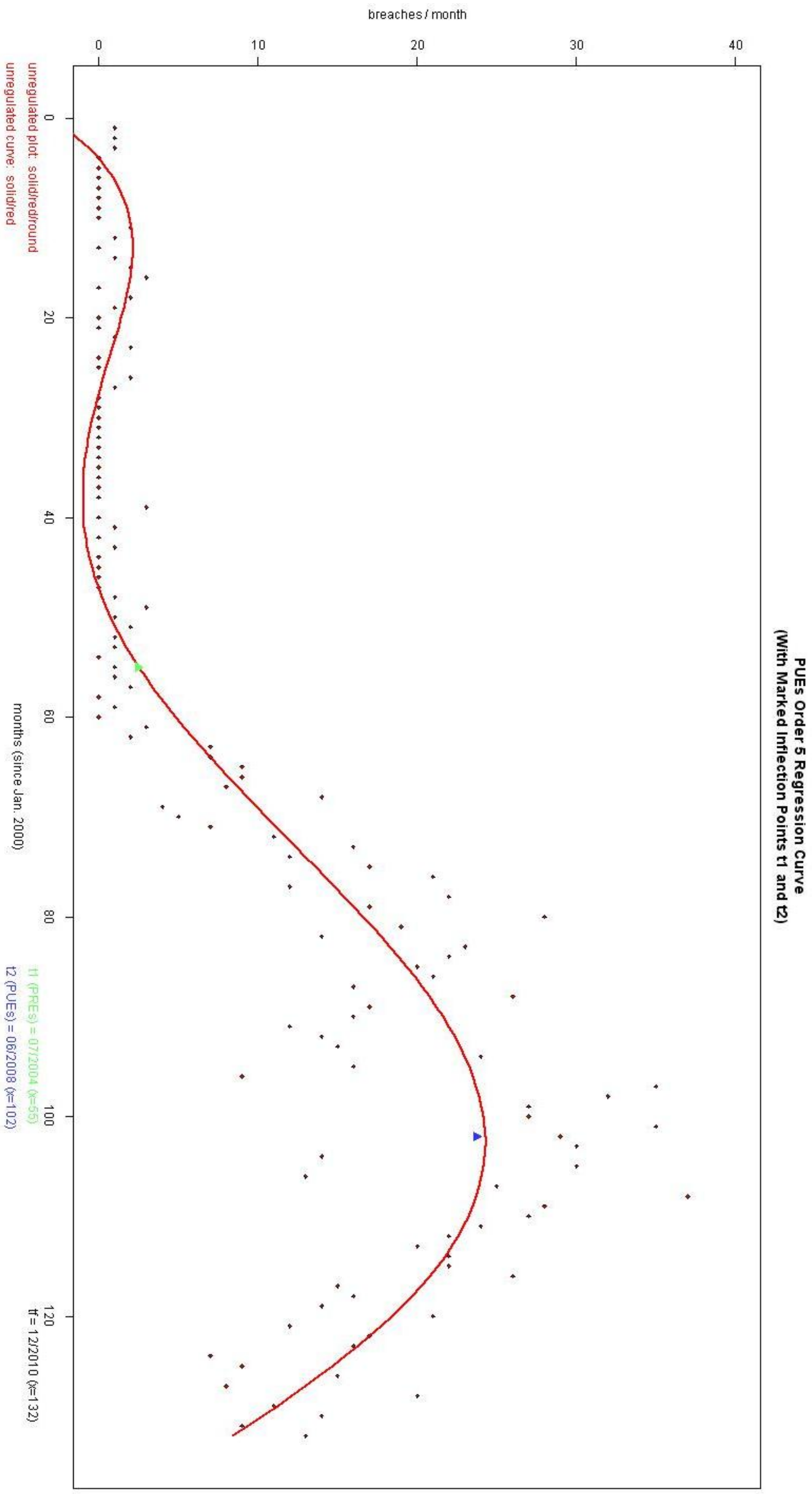
6.3 APPENDIX A.2 – POLYNOMIAL REGRESSIONS OF BREACH INCIDENCE IN PREVIOUSLY UNREGULATED ENTITIES (PUES)


Previously Unregulated Entities (PUEs) - Breach Incidence
breaches / month
0
10
20
30
40
months (since Jan. 2000)
0
20
40
60
80
100
120
order 2: dashed/yellow
order 3: dashed/red
order 4: dashed/green
order 5: dashed/blue
order 6: solid/brown
order 7: solid/purple
order 8: solid/black
order 9: solid/pink
order 10: solid/orange
t1 (PREs) = 07/2004 (x=55)
t2 (PUEs) = 06/2008 (x=102)
tf = 12/2010 (x=132)

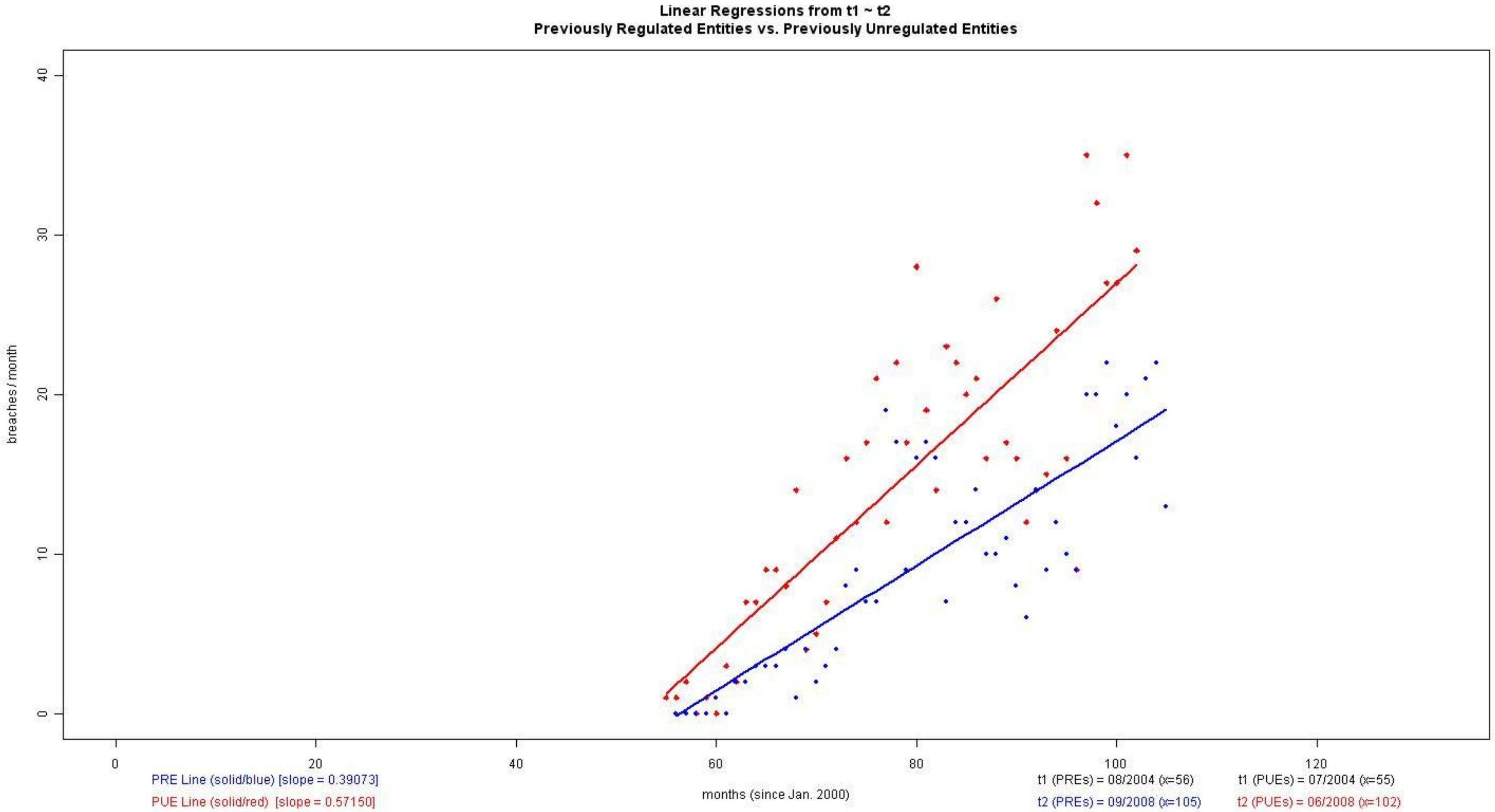
6.4 *Appendix A.3 – Polynomial Regression of Breach Incidence in Previously Regulated Entities (PREs) Using Order 5 Polynomial with Marked Points* T_1 *and* T_2


PREs Order 5 Regression Curve
(With Marked Inflection Points t1 and t2)
breaches / month
0
10
20
30
40
0
20
40
60
80
100
120
months (since Jan. 2000)
regulated plot: solid/blue/diamond
regulated curve: solid/blue
t1 (PRE) = 08/2004 (x=56)
t2 (PRE) = 09/2008 (x=105)
tf = 12/2010 (x=132)

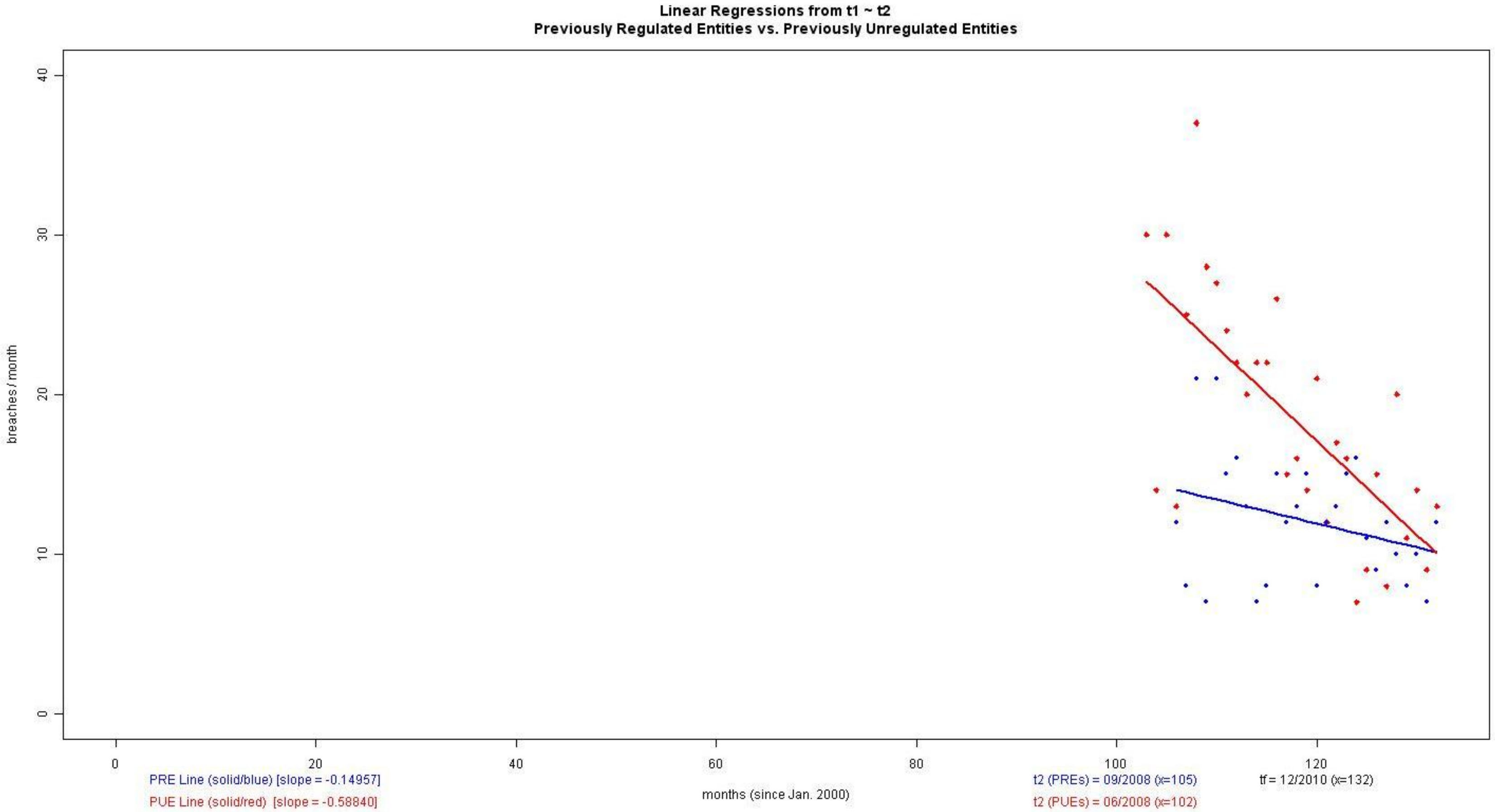
6.5 *Appendix A.4 – Polynomial Regressions of Breach Incidence in Previously Unregulated Entities (PUEs) Using Order 5 Polynomial with Marked Points* T_1 *and* T_2


PUEs Order 5 Regression Curve
(With Marked Inflection Points t1 and t2)
breaches / month
0
10
20
30
40
0
20
40
60
80
100
120
months (since Jan. 2000)
unregulated plot: solid/red/round
unregulated curve: solid/red
t1 (PREs) = 07/2004 (x=55)
t2 (PUEs) = 06/2008 (x=102)
tf = 12/2010 (x=132)

6.6 *APPENDIX A.5 – LINEAR REGRESSIONS OF BREACH INCIDENCE FROM* T$_1$ *TO* T$_2$


Linear Regressions from t1 ~ t2
Previously Regulated Entities vs. Previously Unregulated Entities
breaches / month
0
10
20
30
40
0
20
40
60
80
100
120
months (since Jan. 2000)
PRE Line (solid/blue) [slope = 0.39073]
PUE Line (solid/red) [slope = 0.57150]
t1 (PREs) = 08/2004 (x=56)
t2 (PREs) = 09/2008 (x=105)
t1 (PUEs) = 07/2004 (x=55)
t2 (PUEs) = 06/2008 (x=102)

6.7 *APPENDIX A.6 – LINEAR REGRESSIONS OF BREACH INCIDENCE FROM* T$_2$ *TO* T$_F$


Linear Regressions from t1 ~ t2
Previously Regulated Entities vs. Previously Unregulated Entities
breaches / month
0
10
20
30
40
0
20
40
60
80
100
120
months (since Jan. 2000)
PRE Line (solid/blue) [slope = -0.14957]
PUE Line (solid/red) [slope = -0.58840]
t2 (PREs) = 09/2008 (x=105)
t2 (PUEs) = 06/2008 (x=102)
tf = 12/2010 (x=132)

6.8 *Appendix B.1 – Raw Data Results of Polynomial Regressions for Previously Regulated Entities (PREs)*

```
Call:
lm(formula = breaches ~ poly(dates, 10, raw = TRUE), data =
regulated_dataframe)

Residuals:
    Min      1Q  Median      3Q     Max 
-8.0863 -0.7106 -0.1363  0.9475 10.2255 

Coefficients:
                                Estimate Std. Error t value Pr(>|t|)
(Intercept)                   -1.411e+00  3.768e+00  -0.375    0.709
poly(dates, 10, raw = TRUE)1   8.973e-01  1.855e+00   0.484    0.630
poly(dates, 10, raw = TRUE)2  -1.509e-01  3.033e-01  -0.498    0.620
poly(dates, 10, raw = TRUE)3   1.116e-02  2.341e-02   0.477    0.634
poly(dates, 10, raw = TRUE)4  -4.338e-04  1.004e-03  -0.432    0.666
poly(dates, 10, raw = TRUE)5   9.712e-06  2.597e-05   0.374    0.709
poly(dates, 10, raw = TRUE)6  -1.315e-07  4.216e-07  -0.312    0.756
poly(dates, 10, raw = TRUE)7   1.096e-09  4.321e-09   0.254    0.800
poly(dates, 10, raw = TRUE)8  -5.508e-12  2.713e-11  -0.203    0.839
poly(dates, 10, raw = TRUE)9   1.532e-14  9.520e-14   0.161    0.872
poly(dates, 10, raw = TRUE)10 -1.813e-17  1.430e-16  -0.127    0.899

Residual standard error: 3.082 on 121 degrees of freedom
Multiple R-squared: 0.8133,   Adjusted R-squared: 0.7978 
F-statistic:  52.7 on 10 and 121 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 9, raw = TRUE), data =
regulated_dataframe)

Residuals:
    Min      1Q  Median      3Q     Max 
-8.1123 -0.7132 -0.1446  0.9242 10.2213 

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)
(Intercept)                 -1.175e+00  3.260e+00  -0.360    0.719
poly(dates, 9, raw = TRUE)1  7.351e-01  1.339e+00   0.549    0.584
poly(dates, 9, raw = TRUE)2 -1.201e-01  1.810e-01  -0.663    0.508
poly(dates, 9, raw = TRUE)3  8.572e-03  1.141e-02   0.751    0.454
poly(dates, 9, raw = TRUE)4 -3.167e-04  3.928e-04  -0.806    0.422
poly(dates, 9, raw = TRUE)5  6.578e-06  7.959e-06   0.826    0.410
poly(dates, 9, raw = TRUE)6 -7.948e-08  9.747e-08  -0.815    0.416
poly(dates, 9, raw = TRUE)7  5.553e-10  7.085e-10   0.784    0.435
poly(dates, 9, raw = TRUE)8 -2.086e-12  2.812e-12  -0.742    0.460
poly(dates, 9, raw = TRUE)9  3.265e-15  4.692e-15   0.696    0.488

Residual standard error: 3.069 on 122 degrees of freedom
Multiple R-squared: 0.8132,   Adjusted R-squared: 0.7995 
F-statistic: 59.03 on 9 and 122 DF,  p-value: < 2.2e-16
```

```
Call:
lm(formula = breaches ~ poly(dates, 8, raw = TRUE), data =
regulated_dataframe)

Residuals:
    Min      1Q  Median      3Q     Max 
-8.2128 -0.6477 -0.1000  0.8734 10.4323 

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)
(Intercept)                 -3.495e-02  2.813e+00  -0.012    0.990
poly(dates, 8, raw = TRUE)1  7.464e-02  9.428e-01   0.079    0.937
poly(dates, 8, raw = TRUE)2 -1.659e-02  1.030e-01  -0.161    0.872
poly(dates, 8, raw = TRUE)3  1.492e-03  5.159e-03   0.289    0.773
poly(dates, 8, raw = TRUE)4 -6.081e-05  1.378e-04  -0.441    0.660
poly(dates, 8, raw = TRUE)5  1.234e-06  2.089e-06   0.590    0.556
poly(dates, 8, raw = TRUE)6 -1.282e-08  1.802e-08  -0.712    0.478
poly(dates, 8, raw = TRUE)7  6.562e-11  8.229e-11   0.797    0.427
poly(dates, 8, raw = TRUE)8 -1.315e-13  1.544e-13  -0.852    0.396

Residual standard error: 3.063 on 123 degrees of freedom
Multiple R-squared: 0.8125,   Adjusted R-squared: 0.8003 
F-statistic: 66.62 on 8 and 123 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 7, raw = TRUE), data =
regulated_dataframe)

Residuals:
    Min      1Q  Median      3Q     Max 
-7.9482 -0.8100 -0.1080  0.9637 10.3786 

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)
(Intercept)                  1.195e+00  2.412e+00   0.495    0.621
poly(dates, 7, raw = TRUE)1 -5.130e-01  6.419e-01  -0.799    0.426
poly(dates, 7, raw = TRUE)2  5.753e-02  5.498e-02   1.046    0.297
poly(dates, 7, raw = TRUE)3 -2.516e-03  2.112e-03  -1.191    0.236
poly(dates, 7, raw = TRUE)4  5.103e-05  4.178e-05   1.221    0.224
poly(dates, 7, raw = TRUE)5 -5.055e-07  4.420e-07  -1.144    0.255
poly(dates, 7, raw = TRUE)6  2.392e-09  2.375e-09   1.007    0.316
poly(dates, 7, raw = TRUE)7 -4.331e-12  5.089e-12  -0.851    0.396

Residual standard error: 3.059 on 124 degrees of freedom
Multiple R-squared: 0.8114,   Adjusted R-squared: 0.8007 
F-statistic: 76.21 on 7 and 124 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 6, raw = TRUE), data =
regulated_dataframe)
```

```
Residuals:
     Min       1Q   Median       3Q      Max 
-8.05497 -0.92693 -0.07623  0.70358 10.61856 

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)  
(Intercept)                  1.098e-01  2.045e+00   0.054   0.9573  
poly(dates, 6, raw = TRUE)1 -9.848e-02  4.178e-01  -0.236   0.8140  
poly(dates, 6, raw = TRUE)2  1.678e-02  2.699e-02   0.622   0.5352  
poly(dates, 6, raw = TRUE)3 -8.375e-04  7.567e-04  -1.107   0.2705  
poly(dates, 6, raw = TRUE)4  1.657e-05  1.031e-05   1.607   0.1106  
poly(dates, 6, raw = TRUE)5 -1.338e-07  6.725e-08  -1.989   0.0489 *
poly(dates, 6, raw = TRUE)6  3.756e-10  1.680e-10   2.236   0.0271 *
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 3.056 on 125 degrees of freedom
Multiple R-squared: 0.8103,   Adjusted R-squared: 0.8012 
F-statistic: 88.98 on 6 and 125 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 5, raw = TRUE), data = 
regulated_dataframe)

Residuals:
     Min       1Q   Median       3Q      Max 
-7.94283 -1.44380 -0.07297  0.94290 10.27801 

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)    
(Intercept)                 -2.405e+00  1.735e+00  -1.386 0.168055    
poly(dates, 5, raw = TRUE)1  6.398e-01  2.601e-01   2.460 0.015244 *  
poly(dates, 5, raw = TRUE)2 -3.748e-02  1.200e-02  -3.122 0.002227 ** 
poly(dates, 5, raw = TRUE)3  7.787e-04  2.279e-04   3.417 0.000852 ***
poly(dates, 5, raw = TRUE)4 -6.118e-06  1.886e-06  -3.244 0.001508 ** 
poly(dates, 5, raw = TRUE)5  1.613e-08  5.644e-09   2.857 0.005003 ** 
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 3.104 on 126 degrees of freedom
Multiple R-squared: 0.8027,   Adjusted R-squared: 0.7949 
F-statistic: 102.5 on 5 and 126 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 4, raw = TRUE), data = 
regulated_dataframe)

Residuals:
     Min       1Q   Median       3Q      Max 
-8.60235 -1.44455 -0.07203  0.62101 10.95400 

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)
```

```
(Intercept)                  4.633e-01  1.454e+00   0.319 0.750541
poly(dates, 4, raw = TRUE)1  2.529e-02  1.503e-01   0.168 0.866616
poly(dates, 4, raw = TRUE)2 -5.621e-03  4.570e-03  -1.230 0.220981
poly(dates, 4, raw = TRUE)3  1.436e-04  5.154e-05   2.787 0.006144 **
poly(dates, 4, raw = TRUE)4 -7.567e-07  1.923e-07  -3.936 0.000136 ***
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 3.19 on 127 degrees of freedom
Multiple R-squared: 0.7899,   Adjusted R-squared: 0.7833
F-statistic: 119.4 on 4 and 127 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 3, raw = TRUE), data =
regulated_dataframe)

Residuals:
    Min      1Q  Median      3Q     Max
-7.1992 -2.4464 -0.1496  1.6829 10.0262

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)
(Intercept)                  4.000e+00  1.206e+00   3.317  0.00119 **
poly(dates, 3, raw = TRUE)1 -4.892e-01  7.824e-02  -6.252 5.56e-09 ***
poly(dates, 3, raw = TRUE)2  1.163e-02  1.364e-03   8.527 3.63e-14 ***
poly(dates, 3, raw = TRUE)3 -5.767e-05  6.744e-06  -8.552 3.17e-14 ***
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 3.366 on 128 degrees of freedom
Multiple R-squared: 0.7643,   Adjusted R-squared: 0.7588
F-statistic: 138.3 on 3 and 128 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 2, raw = TRUE), data =
regulated_dataframe)

Residuals:
    Min      1Q  Median      3Q     Max
-8.6469 -2.8902 -0.6383  1.8316 11.5419

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)
(Intercept)                 -2.9370362  1.1143923  -2.636  0.00943 **
poly(dates, 2, raw = TRUE)1  0.1252209  0.0386824   3.237  0.00153 **
poly(dates, 2, raw = TRUE)2  0.0001270  0.0002817   0.451  0.65283
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 4.203 on 129 degrees of freedom
Multiple R-squared: 0.6296,   Adjusted R-squared: 0.6239
F-statistic: 109.6 on 2 and 129 DF,  p-value: < 2.2e-16
```

6.9 APPENDIX B.2 – RAW DATA RESULTS OF POLYNOMIAL REGRESSIONS FOR PREVIOUSLY UNREGULATED ENTITIES (PUES)

```
Call:
lm(formula = breaches ~ poly(dates, 10, raw = TRUE), data =
unregulated_dataframe)

Residuals:
     Min       1Q   Median       3Q      Max
-14.5137  -1.2929  -0.0475   1.7185  11.9182

Coefficients:
                                Estimate Std. Error t value Pr(>|t|)
(Intercept)                   -1.254e+00  5.221e+00  -0.240    0.811
poly(dates, 10, raw = TRUE)1   1.360e+00  2.571e+00   0.529    0.598
poly(dates, 10, raw = TRUE)2  -2.761e-01  4.202e-01  -0.657    0.512
poly(dates, 10, raw = TRUE)3   2.412e-02  3.244e-02   0.744    0.459
poly(dates, 10, raw = TRUE)4  -1.091e-03  1.391e-03  -0.784    0.434
poly(dates, 10, raw = TRUE)5   2.820e-05  3.599e-05   0.784    0.435
poly(dates, 10, raw = TRUE)6  -4.391e-07  5.842e-07  -0.752    0.454
poly(dates, 10, raw = TRUE)7   4.193e-09  5.987e-09   0.700    0.485
poly(dates, 10, raw = TRUE)8  -2.396e-11  3.759e-11  -0.638    0.525
poly(dates, 10, raw = TRUE)9   7.501e-14  1.319e-13   0.569    0.571
poly(dates, 10, raw = TRUE)10 -9.838e-17  1.981e-16  -0.497    0.620

Residual standard error: 4.27 on 121 degrees of freedom
Multiple R-squared: 0.8425,   Adjusted R-squared: 0.8295
F-statistic: 64.75 on 10 and 121 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 9, raw = TRUE), data =
unregulated_dataframe)

Residuals:
      Min        1Q    Median        3Q       Max
-14.47765  -1.17216  -0.02358   1.60097  12.06985

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)
(Intercept)                  2.906e-02  4.522e+00   0.006    0.995
poly(dates, 9, raw = TRUE)1  4.805e-01  1.857e+00   0.259    0.796
poly(dates, 9, raw = TRUE)2 -1.090e-01  2.511e-01  -0.434    0.665
poly(dates, 9, raw = TRUE)3  1.007e-02  1.583e-02   0.636    0.526
poly(dates, 9, raw = TRUE)4 -4.557e-04  5.447e-04  -0.836    0.405
poly(dates, 9, raw = TRUE)5  1.119e-05  1.104e-05   1.014    0.313
poly(dates, 9, raw = TRUE)6 -1.569e-07  1.352e-07  -1.161    0.248
poly(dates, 9, raw = TRUE)7  1.260e-09  9.826e-10   1.282    0.202
poly(dates, 9, raw = TRUE)8 -5.399e-12  3.900e-12  -1.384    0.169
poly(dates, 9, raw = TRUE)9  9.585e-15  6.507e-15   1.473    0.143

Residual standard error: 4.257 on 122 degrees of freedom
Multiple R-squared: 0.8422,   Adjusted R-squared: 0.8306
```

```
F-statistic: 72.36 on 9 and 122 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 8, raw = TRUE), data =
unregulated_dataframe)

Residuals:
    Min      1Q  Median      3Q     Max
-15.100  -1.488   0.181   1.678  12.204

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)
(Intercept)                  3.375e+00  3.928e+00   0.859    0.392
poly(dates, 8, raw = TRUE)1 -1.459e+00  1.317e+00  -1.108    0.270
poly(dates, 8, raw = TRUE)2  1.949e-01  1.438e-01   1.355    0.178
poly(dates, 8, raw = TRUE)3 -1.071e-02  7.203e-03  -1.487    0.140
poly(dates, 8, raw = TRUE)4  2.956e-04  1.924e-04   1.536    0.127
poly(dates, 8, raw = TRUE)5 -4.495e-06  2.918e-06  -1.541    0.126
poly(dates, 8, raw = TRUE)6  3.873e-08  2.516e-08   1.539    0.126
poly(dates, 8, raw = TRUE)7 -1.779e-10  1.149e-10  -1.548    0.124
poly(dates, 8, raw = TRUE)8  3.381e-13  2.156e-13   1.569    0.119

Residual standard error: 4.277 on 123 degrees of freedom
Multiple R-squared: 0.8394,   Adjusted R-squared: 0.829
F-statistic: 80.37 on 8 and 123 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 7, raw = TRUE), data =
unregulated_dataframe)

Residuals:
     Min       1Q   Median       3Q      Max
-15.5820  -0.9497   0.0247   1.4539  12.8649

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)
(Intercept)                  2.125e-01  3.391e+00   0.063    0.950
poly(dates, 7, raw = TRUE)1  5.254e-02  9.027e-01   0.058    0.954
poly(dates, 7, raw = TRUE)2  4.281e-03  7.731e-02   0.055    0.956
poly(dates, 7, raw = TRUE)3 -4.067e-04  2.970e-03  -0.137    0.891
poly(dates, 7, raw = TRUE)4  7.965e-06  5.875e-05   0.136    0.892
poly(dates, 7, raw = TRUE)5 -2.251e-08  6.215e-07  -0.036    0.971
poly(dates, 7, raw = TRUE)6 -3.898e-10  3.340e-09  -0.117    0.907
poly(dates, 7, raw = TRUE)7  2.021e-12  7.157e-12   0.282    0.778

Residual standard error: 4.302 on 124 degrees of freedom
Multiple R-squared: 0.8362,   Adjusted R-squared: 0.827
F-statistic: 90.44 on 7 and 124 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 6, raw = TRUE), data =
unregulated_dataframe)
```

```
Residuals:
     Min       1Q   Median       3Q      Max 
-15.5395  -0.9556   0.0204   1.4732  12.9893 

Coefficients:
                             Estimate Std. Error t value Pr(>|t|)  
(Intercept)                 7.188e-01  2.868e+00   0.251   0.8025  
poly(dates, 6, raw = TRUE)1 -1.408e-01  5.859e-01  -0.240   0.8104  
poly(dates, 6, raw = TRUE)2  2.329e-02  3.785e-02   0.615   0.5394  
poly(dates, 6, raw = TRUE)3 -1.190e-03  1.061e-03  -1.121   0.2644  
poly(dates, 6, raw = TRUE)4  2.404e-05  1.446e-05   1.662   0.0990 .
poly(dates, 6, raw = TRUE)5 -1.960e-07  9.431e-08  -2.078   0.0398 *
poly(dates, 6, raw = TRUE)6  5.509e-10  2.356e-10   2.339   0.0209 *
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 4.286 on 125 degrees of freedom
Multiple R-squared: 0.8361,   Adjusted R-squared: 0.8282 
F-statistic: 106.3 on 6 and 125 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 5, raw = TRUE), data = 
unregulated_dataframe)

Residuals:
     Min       1Q   Median       3Q      Max 
-14.5072  -1.7734   0.2465   1.6417  13.2923 

Coefficients:
                             Estimate Std. Error t value Pr(>|t|)    
(Intercept)                -2.969e+00  2.437e+00  -1.218 0.225405    
poly(dates, 5, raw = TRUE)1  9.419e-01  3.654e-01   2.578 0.011100 *  
poly(dates, 5, raw = TRUE)2 -5.628e-02  1.687e-02  -3.337 0.001115 ** 
poly(dates, 5, raw = TRUE)3  1.180e-03  3.202e-04   3.687 0.000336 ***
poly(dates, 5, raw = TRUE)4 -9.231e-06  2.650e-06  -3.484 0.000680 ***
poly(dates, 5, raw = TRUE)5  2.383e-08  7.930e-09   3.005 0.003202 ** 
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 4.361 on 126 degrees of freedom
Multiple R-squared: 0.8289,   Adjusted R-squared: 0.8221 
F-statistic: 122.1 on 5 and 126 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 4, raw = TRUE), data = 
unregulated_dataframe)

Residuals:
      Min        1Q    Median        3Q       Max 
-13.76136  -1.84406   0.04996   1.95247  12.56933 

Coefficients:
```

```
                              Estimate Std. Error t value Pr(>|t|)    
(Intercept)                  1.270e+00  2.050e+00   0.620  0.53660    
poly(dates, 4, raw = TRUE)1  3.366e-02  2.118e-01   0.159  0.87399    
poly(dates, 4, raw = TRUE)2 -9.194e-03  6.442e-03  -1.427  0.15599    
poly(dates, 4, raw = TRUE)3  2.419e-04  7.264e-05   3.330  0.00114 ** 
poly(dates, 4, raw = TRUE)4 -1.307e-06  2.710e-07  -4.823 3.97e-06 ***
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 4.497 on 127 degrees of freedom
Multiple R-squared: 0.8167,   Adjusted R-squared: 0.8109 
F-statistic: 141.4 on 4 and 127 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 3, raw = TRUE), data = 
unregulated_dataframe)

Residuals:
     Min       1Q   Median       3Q      Max 
-12.6299  -3.4549   0.4911   2.7258  14.8505 

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)    
(Intercept)                  7.380e+00  1.746e+00   4.227 4.47e-05 ***
poly(dates, 3, raw = TRUE)1 -8.549e-01  1.132e-01  -7.549 7.24e-12 ***
poly(dates, 3, raw = TRUE)2  2.061e-02  1.975e-03  10.436  < 2e-16 ***
poly(dates, 3, raw = TRUE)3 -1.058e-04  9.761e-06 -10.838  < 2e-16 ***
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 4.873 on 128 degrees of freedom
Multiple R-squared: 0.7831,   Adjusted R-squared: 0.778 
F-statistic:   154 on 3 and 128 DF,  p-value: < 2.2e-16


Call:
lm(formula = breaches ~ poly(dates, 2, raw = TRUE), data = 
unregulated_dataframe)

Residuals:
     Min       1Q   Median       3Q      Max 
-13.7446  -4.7826  -0.6609   3.9663  18.7623 

Coefficients:
                              Estimate Std. Error t value Pr(>|t|)    
(Intercept)                 -5.3467811  1.7820016  -3.000  0.00324 ** 
poly(dates, 2, raw = TRUE)1  0.2721034  0.0618562   4.399 2.25e-05 ***
poly(dates, 2, raw = TRUE)2 -0.0004975  0.0004505  -1.104  0.27155    
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 6.721 on 129 degrees of freedom
Multiple R-squared: 0.5841,   Adjusted R-squared: 0.5776 
F-statistic: 90.57 on 2 and 129 DF,  p-value: < 2.2e-16
```

6.10 APPENDIX B.3 – RAW DATA RESULTS OF LINEAR REGRESSIONS FOR PREs AND PUEs FROM T_1 TO T_2

```
Call:
lm(formula = breaches ~ dates, data = PRE_dataframe_t1_t2)

Residuals:
    Min      1Q  Median      3Q     Max 
-7.5627 -2.1040 -0.3573  1.9274 10.9076 

Coefficients:
             Estimate Std. Error t value Pr(>|t|)    
(Intercept) -21.99395    3.10995  -7.072 5.70e-09 ***
dates         0.39073    0.03803  10.275 1.03e-13 ***
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 3.88 on 48 degrees of freedom
Multiple R-squared: 0.6875,   Adjusted R-squared: 0.6809 
F-statistic: 105.6 on 1 and 48 DF,  p-value: 1.034e-13


Call:
lm(formula = breaches ~ dates, data = PUE_dataframe_t1_t2)

Residuals:
      Min        1Q    Median        3Q       Max 
-15.68845  -3.29387   0.02638   3.20518  12.45528 

Coefficients:
            Estimate Std. Error t value Pr(>|t|)    
(Intercept) -30.1739     4.5121  -6.687 2.69e-08 ***
dates         0.5715     0.0566  10.096 3.00e-13 ***
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 5.433 on 46 degrees of freedom
Multiple R-squared: 0.689,    Adjusted R-squared: 0.6823 
F-statistic: 101.9 on 1 and 46 DF,  p-value: 3.001e-13


Call:
lm(formula = breaches ~ dates, data = PRE_dataframe_t2_tf)

Residuals:
     Min       1Q   Median       3Q      Max 
-6.56980 -2.30271  0.02849  2.17379  7.57977 

Coefficients:
            Estimate Std. Error t value Pr(>|t|)  
(Intercept) 29.87322   11.07548   2.697   0.0123 *
dates       -0.14957    0.09287  -1.611   0.1198  
---
```

```
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 3.759 on 25 degrees of freedom
Multiple R-squared: 0.094,    Adjusted R-squared: 0.05776
F-statistic: 2.594 on 1 and 25 DF,  p-value: 0.1198


Call:
lm(formula = breaches ~ dates, data = PUE_dataframe_t2_tf)

Residuals:
     Min       1Q   Median       3Q      Max
-12.5105  -3.3311   0.8755   2.9495  12.8432

Coefficients:
            Estimate Std. Error t value Pr(>|t|)
(Intercept)  87.7074    13.6861   6.408 6.14e-07 ***
dates        -0.5884     0.1162  -5.066 2.32e-05 ***
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 5.507 on 28 degrees of freedom
Multiple R-squared: 0.4782,   Adjusted R-squared: 0.4596
F-statistic: 25.66 on 1 and 28 DF,  p-value: 2.318e-05
```

6.11 Appendix B.4 – Raw Data Results of Differential Running Averages Method (Method 3)

```
maxDiff: 29.952777777777776
maxDiffCounter: 72
Ma_final: 0.5972222222222222
Mb_final: 12.783333333333333
Mc_final: 1.75
Md_final: 19.516666666666666
diffReg_final: 12.186111111111112
diffUnreg_final: 17.766666666666666

xa: 36.0
xb: 102.0
Sr: 0.18463804713804716
Su: 0.2691919191919192

maxDiffCounter: 72 --> 12/1/2005

Ma: regulated avg. before t0
Mb: regulated avg. after t0

Mc: unregulated avg. before t0
Md: unregulated avg. after t0
```

6.12 Appendix C.1 – R Code for Polynomial Regression Analysis

```
# import database file -----------------------------------------------
--

dataloss_monthly <- read.table(file("c:\\my
documents\\+classes\\+dissertation\\data\\dataloss_monthly.csv"),
header = TRUE, sep = ",");


# extract monthly totals ---------------------------------------------
----

dataloss_monthly_regulatedTotal <- dataloss_monthly[5];
dataloss_monthly_unregulatedTotal <- dataloss_monthly[6];

dates <- c(1:132);

# create dataframes -------------------------------------------------

regulated_breaches <- dataloss_monthly_regulatedTotal[1:132,1];
regulated_dataframe <- data.frame(dates, regulated_breaches);

unregulated_breaches <- dataloss_monthly_unregulatedTotal[1:132,1];
unregulated_dataframe <- data.frame(dates, unregulated_breaches);

names(regulated_dataframe) <- c("dates", "breaches");
names(unregulated_dataframe) <- c("dates", "breaches");


# polynomial regressions ---------------------------------------------
----

regulated_poly10_full <- lm(breaches ~ poly(dates,10,raw=TRUE),
regulated_dataframe);
regulated_poly9_full <- lm(breaches ~ poly(dates,9,raw=TRUE),
regulated_dataframe);
regulated_poly8_full <- lm(breaches ~ poly(dates,8,raw=TRUE),
regulated_dataframe);
regulated_poly7_full <- lm(breaches ~ poly(dates,7,raw=TRUE),
regulated_dataframe);

regulated_poly6_full <- lm(breaches ~ poly(dates,6,raw=TRUE),
regulated_dataframe);
regulated_poly5_full <- lm(breaches ~ poly(dates,5,raw=TRUE),
regulated_dataframe);
regulated_poly4_full <- lm(breaches ~ poly(dates,4,raw=TRUE),
regulated_dataframe);
regulated_poly3_full <- lm(breaches ~ poly(dates,3,raw=TRUE),
regulated_dataframe);
regulated_poly2_full <- lm(breaches ~ poly(dates,2,raw=TRUE),
regulated_dataframe);
```

```
unregulated_poly10_full <- lm(breaches ~ poly(dates,10,raw=TRUE),
unregulated_dataframe);
unregulated_poly9_full <- lm(breaches ~ poly(dates,9,raw=TRUE),
unregulated_dataframe);
unregulated_poly8_full <- lm(breaches ~ poly(dates,8,raw=TRUE),
unregulated_dataframe);
unregulated_poly7_full <- lm(breaches ~ poly(dates,7,raw=TRUE),
unregulated_dataframe);

unregulated_poly6_full <- lm(breaches ~ poly(dates,6,raw=TRUE),
unregulated_dataframe);
unregulated_poly5_full <- lm(breaches ~ poly(dates,5,raw=TRUE),
unregulated_dataframe);
unregulated_poly4_full <- lm(breaches ~ poly(dates,4,raw=TRUE),
unregulated_dataframe);
unregulated_poly3_full <- lm(breaches ~ poly(dates,3,raw=TRUE),
unregulated_dataframe);
unregulated_poly2_full <- lm(breaches ~ poly(dates,2,raw=TRUE),
unregulated_dataframe);


# setup multiple plot --------------------------------------------------
-

#par(mfrow=c(2,1));

# plot PREs polynomial regressions ------------------------------------
--------------

jpeg("c:\\my
documents\\+classes\\+dissertation\\data\\polynomial_regressions_PREs.j
pg", width=1440, height = 785);

plot(dates,dummy_plot,pch=21,bg='#000000',cex=0, xlab="months (since
Jan. 2000)", ylab="breaches / month", main="Previously Regulated
Entities (PREs) - Breach Incidence", xlim=c(0,132), ylim=c(0,40));

points(dates,regulated_breaches,pch=21,bg='#0000FF',cex=0.5);

lines(dates, predict(regulated_poly10_full), lwd=2, lty=1,
col='orange');
lines(dates, predict(regulated_poly9_full), lwd=2, lty=1, col='pink');
lines(dates, predict(regulated_poly8_full), lwd=2, lty=1, col='black');
lines(dates, predict(regulated_poly7_full), lwd=2, lty=1,
col='purple');

lines(dates, predict(regulated_poly6_full), lwd=2, lty=1, col='brown');
lines(dates, predict(regulated_poly5_full), lwd=2, lty=3, col='blue');
lines(dates, predict(regulated_poly4_full), lwd=2, lty=3, col='green');
lines(dates, predict(regulated_poly3_full), lwd=2, lty=3, col='red');
lines(dates, predict(regulated_poly2_full), lwd=2, lty=3,
col='yellow');

mtext("order 10:  solid/orange", side=3, at=4.8, line=-10,
col='orange');
```

```
mtext("order 9:  solid/pink", side=3, at=3.7, line=-9, col='pink');
mtext("order 8:  solid/black", side=3, at=4.0, line=-8, col='black');
mtext("order 7:  solid/purple", side=3, at=4.3, line=-7, col='purple');

mtext("order 6:  solid/brown", side=3, at=4.2, line=-6, col='brown');
mtext("order 5:  dashed/blue", side=3, at=4.5, line=-5, col='blue');
mtext("order 4:  dashed/green", side=3, at=4.9, line=-4, col='green');
mtext("order 3:  dashed/red", side=3, at=4.2, line=-3, col='red');
mtext("order 2:  dashed/yellow", side=3, at=5, line=-2, col='yellow');

# mtext("dates:  t1 = 54; t2(PREs) = 103; t2(PUEs) = 105", side=1,
at=67, line=4, col='#000000');

mtext("t1 (PRE) = 08/2004 (x=56)", side=1, at=93, line=2,
col='#66FF66');
mtext("t2 (PRE) = 09/2008 (x=105)", side=1, at=93.2, line=3.5,
col='#FF3333');
mtext("tf = 12/2010 (x=132)", side=1, at=125, line=2, col='#000000');

dev.off();




# plot PUEs polynomial regressions -------------------------------------
--------------

jpeg("c:\\my
documents\\+classes\\+dissertation\\data\\polynomial_regressions_PUEs.j
pg", width=1440, height = 785);

plot(dates,dummy_plot,pch=21,bg='#000000',cex=0, xlab="months (since
Jan. 2000)", ylab="breaches / month", main="Previously Unregulated
Entities (PUEs) - Breach Incidence", xlim=c(0,132), ylim=c(0,40));

points(dates,unregulated_breaches,pch=21,bg='#FF0000',cex=0.5);

lines(dates, predict(unregulated_poly10_full), lwd=2, lty=1,
col='orange');
lines(dates, predict(unregulated_poly9_full), lwd=2, lty=1,
col='pink');
lines(dates, predict(unregulated_poly8_full), lwd=2, lty=1,
col='black');
lines(dates, predict(unregulated_poly7_full), lwd=2, lty=1,
col='purple');

lines(dates, predict(unregulated_poly6_full), lwd=2, lty=1,
col='brown');
lines(dates, predict(unregulated_poly5_full), lwd=2, lty=3,
col='blue');
lines(dates, predict(unregulated_poly4_full), lwd=2, lty=3,
col='green');
lines(dates, predict(unregulated_poly3_full), lwd=2, lty=3, col='red');
lines(dates, predict(unregulated_poly2_full), lwd=2, lty=3,
col='yellow');
```

```
mtext("order 10:  solid/orange", side=3, at=4.8, line=-10,
col='orange');
mtext("order 9:  solid/pink", side=3, at=3.7, line=-9, col='pink');
mtext("order 8:  solid/black", side=3, at=4.0, line=-8, col='black');
mtext("order 7:  solid/purple", side=3, at=4.3, line=-7, col='purple');

mtext("order 6:  solid/brown", side=3, at=4.2, line=-6, col='brown');
mtext("order 5:  dashed/blue", side=3, at=4.5, line=-5, col='blue');
mtext("order 4:  dashed/green", side=3, at=4.9, line=-4, col='green');
mtext("order 3:  dashed/red", side=3, at=4.2, line=-3, col='red');
mtext("order 2:  dashed/yellow", side=3, at=5, line=-2, col='yellow');

mtext("t1 (PREs) = 07/2004 (x=55)", side=1, at=93, line=2,
col='#66FF66');
mtext("t2 (PUEs) = 06/2008 (x=102)", side=1, at=93.2, line=3.5,
col='#3333FF');
mtext("tf = 12/2010 (x=132)", side=1, at=125, line=2, col='#000000');

dev.off();



# plot PRE/order 5 regression curve ----------------------------------
---------------

jpeg("c:\\my
documents\\+classes\\+dissertation\\data\\polynomial_regressions_PREs_o
rder5.jpg", width=1440, height = 785);

plot(dates,regulated_breaches,pch=21,bg='#0000FF',cex=0.5, xlab="months
(since Jan. 2000)", ylab="breaches / month", main="PREs Order 5
Regression Curve\n(With Marked Inflection Points t1 and t2)", sub="",
cex.sub=0.75, xlim=c(0,132), ylim=c(0,40));

lines(dates, predict(regulated_poly5_full), lwd=2, lty=1,
col='#0000FF');

points(56,1.35455,pch=17,col='#66FF66',cex=1.5)
points(105,15.21707,pch=17,col='#FF3333',cex=1.5)

mtext("regulated plot:  solid/blue/diamond", side=1, at=5, line=2,
col='#0000FF');
mtext("regulated curve:  solid/blue", side=1, at=2.7, line=3.5,
col='#0000FF');


mtext("t1 (PRE) = 08/2004 (x=56)", side=1, at=93, line=2,
col='#66FF66');
mtext("t2 (PRE) = 09/2008 (x=105)", side=1, at=93.2, line=3.5,
col='#FF3333');
mtext("tf = 12/2010 (x=132)", side=1, at=125, line=2, col='#000000');


dev.off();
```

```
# plot PUE/order 5 regression curve ------------------------------------
---------------

jpeg("c:\\my
documents\\+classes\\+dissertation\\data\\polynomial_regressions_PUEs_o
rder5.jpg", width=1440, height = 785);

plot(dates,unregulated_breaches,pch=23,bg='#FF0000',cex=0.5,
xlab="months (since Jan. 2000)", ylab="breaches / month", main="PUEs
Order 5 Regression Curve\n(With Marked Inflection Points t1 and t2)",
sub="", cex.sub=0.75, xlim=c(0,132), ylim=c(0,40));

lines(dates, predict(unregulated_poly5_full), lwd=2, lty=1,
col='#FF0000');

points(55,2.43484,pch=17,col='#66FF66',cex=1.50)
points(102,23.70245,pch=17,col='#3333FF',cex=1.50)

mtext("unregulated plot:  solid/red/round", side=1, at=4.1, line=2,
col='#FF0000');
mtext("unregulated curve:  solid/red", side=1, at=2.7, line=3.5,
col='#FF0000');

mtext("t1 (PREs) = 07/2004 (x=55)", side=1, at=93, line=2,
col='#66FF66');
mtext("t2 (PUEs) = 06/2008 (x=102)", side=1, at=93.2, line=3.5,
col='#3333FF');
mtext("tf = 12/2010 (x=132)", side=1, at=125, line=2, col='#000000');


dev.off();


# plot order 5/PRE and order 5/PUE regressions combined ---------------
-----------------------------------

#points(dates,unregulated_breaches,pch=23,bg='yellow',cex=0.5);

#lines(dates, predict(unregulated_poly5_full), lwd=2, lty=1,
col='blue');



# print summary statistics - PREs -------------------------------------
-------------

sink("c:\\my
documents\\+classes\\+dissertation\\data\\polynomial_regressions_PREs.t
xt", split=FALSE);

summary(regulated_poly10_full);
summary(regulated_poly9_full);
summary(regulated_poly8_full);
summary(regulated_poly7_full);
summary(regulated_poly6_full);
summary(regulated_poly5_full);
summary(regulated_poly4_full);
summary(regulated_poly3_full);
summary(regulated_poly2_full);

sink();


# print summary statistics - PUEs -------------------------------------
-------------

sink("c:\\my
documents\\+classes\\+dissertation\\data\\polynomial_regressions_PUEs.t
xt", split=FALSE);

summary(unregulated_poly10_full);
summary(unregulated_poly9_full);
summary(unregulated_poly8_full);
summary(unregulated_poly7_full);
summary(unregulated_poly6_full);
summary(unregulated_poly5_full);
summary(unregulated_poly4_full);
summary(unregulated_poly3_full);
summary(unregulated_poly2_full);

sink();
```

6.13 Appendix C.2 – R Code for Linear Regression Analysis

```
# import database file ------------------------------------------------
--

dataloss_monthly <- read.table(file("c:\\my
documents\\+classes\\+dissertation\\data\\dataloss_monthly.csv"),
header = TRUE, sep = ",");


# extract monthly totals ----------------------------------------------
----

dataloss_monthly_PRE <- dataloss_monthly[5];
dataloss_monthly_PUE <- dataloss_monthly[6];

dates <- c(1:132);

dates_PRE_t1_t2 <- c(56:105);
dates_PRE_t2_tf <- c(106:132);

dates_PUE_t1_t2 <- c(55:102);
dates_PUE_t2_tf <- c(103:132);

dates <- c(1:132);


# create dataframes --------------------------------------------------

PRE_breaches_t1_t2 <- dataloss_monthly_PRE[56:105,1];
PRE_dataframe_t1_t2 <- data.frame(dates_PRE_t1_t2, PRE_breaches_t1_t2);

PRE_breaches_t2_tf <- dataloss_monthly_PRE[106:132,1];
PRE_dataframe_t2_tf <- data.frame(dates_PRE_t2_tf, PRE_breaches_t2_tf);

PUE_breaches_t1_t2 <- dataloss_monthly_PUE[55:102,1];
PUE_dataframe_t1_t2 <- data.frame(dates_PUE_t1_t2, PUE_breaches_t1_t2);

PUE_breaches_t2_tf <- dataloss_monthly_PUE[103:132,1];
PUE_dataframe_t2_tf <- data.frame(dates_PUE_t2_tf, PUE_breaches_t2_tf);

names(PRE_dataframe_t1_t2) <- c("dates", "breaches");
names(PRE_dataframe_t2_tf) <- c("dates", "breaches");

names(PUE_dataframe_t1_t2) <- c("dates", "breaches");
names(PUE_dataframe_t2_tf) <- c("dates", "breaches");


# linear regressions --------------------------------------------------

PRE_linear_t1_t2 <- lm(breaches ~ dates, PRE_dataframe_t1_t2);
PRE_linear_t2_tf <- lm(breaches ~ dates, PRE_dataframe_t2_tf);

PUE_linear_t1_t2 <- lm(breaches ~ dates, PUE_dataframe_t1_t2);
```

```
PUE_linear_t2_tf <- lm(breaches ~ dates, PUE_dataframe_t2_tf);


# plot linear regressions t1 ~ t2 ------------------------------------
-------------

jpeg("c:\\my
documents\\+classes\\+dissertation\\data\\linear_regressions_t1_t2.jpg"
, width=1440, height = 785);

# create plot of full range (1 - 132)
plot(dates_PUE_t1_t2,PUE_breaches_t1_t2,pch=23,col='#FF0000',bg='#FF000
0',cex=0.75,xlab="months (since Jan. 2000)", ylab="breaches /
month",main="Linear Regressions from t1 ~ t2\nPreviously Regulated
Entities vs. Previously Unregulated Entities", xlim=c(0,132),
ylim=c(0,40));

points(dates_PRE_t1_t2, PRE_breaches_t1_t2, pch=21, col='#0000FF',
bg='#0000FF', cex=0.75);

lines(dates_PRE_t1_t2, predict(PRE_linear_t1_t2), lwd=2, lty=1,
col='#0000FF');
lines(dates_PUE_t1_t2, predict(PUE_linear_t1_t2), lwd=2, lty=1,
col='#FF0000');

mtext("PRE Line (solid/blue) [slope = 0.39073]", side=1, at=15, line=2,
col='#0000FF');
mtext("PUE Line (solid/red)  [slope = 0.57150]", side=1, at=14.80,
line=3.5, col='#FF0000');

mtext("t1 (PREs) = 08/2004 (x=56)", side=1, at=100, line=2,
col='#000000');
mtext("t2 (PREs) = 09/2008 (x=105)", side=1, at=100.4, line=3.5,
col='#0000FF');
mtext("t1 (PUEs) = 07/2004 (x=55)", side=1, at=120, line=2,
col='#000000');
mtext("t2 (PUEs) = 06/2008 (x=102)", side=1, at=120.4, line=3.5,
col='#FF0000');


dev.off();


# plot linear regressions t2 ~ tf ------------------------------------
-------------

jpeg("c:\\my
documents\\+classes\\+dissertation\\data\\linear_regressions_t2_tf.jpg"
, width=1440, height = 785);

# create plot of full range (1 - 132)
plot(dates_PUE_t2_tf,PUE_breaches_t2_tf,pch=23,col='#FF0000',bg='#FF000
0',cex=0.75,xlab="months (since Jan. 2000)", ylab="breaches /
month",main="Linear Regressions from t1 ~ t2\nPreviously Regulated
Entities vs. Previously Unregulated Entities", xlim=c(0,132),
ylim=c(0,40));

points(dates_PRE_t2_tf, PRE_breaches_t2_tf, pch=21, col='#0000FF',
bg='#0000FF', cex=0.75);

lines(dates_PRE_t2_tf, predict(PRE_linear_t2_tf), lwd=2, lty=1,
col='#0000FF');
lines(dates_PUE_t2_tf, predict(PUE_linear_t2_tf), lwd=2, lty=1,
col='#FF0000');

mtext("PRE Line (solid/blue) [slope = -0.14957]", side=1, at=15,
line=2, col='#0000FF');
mtext("PUE Line (solid/red)  [slope = -0.58840]", side=1, at=14.80,
line=3.5, col='#FF0000');

mtext("t2 (PREs) = 09/2008 (x=105)", side=1, at=100, line=2,
col='#0000FF');
mtext("t2 (PUEs) = 06/2008 (x=102)", side=1, at=100, line=3.5,
col='#FF0000');
mtext("tf = 12/2010 (x=132)", side=1, at=120, line=2, col='#000000');


dev.off();


# linear regression summaries ------------------------------------------
---------

sink("c:\\my
documents\\+classes\\+dissertation\\data\\linear_regressions.txt",
split=FALSE);

summary(PRE_linear_t1_t2);
summary(PUE_linear_t1_t2);

summary(PRE_linear_t2_tf);
summary(PUE_linear_t2_tf);

sink();
```

6.14 *APPENDIX D.1 – JAVA CODE FOR CURVE INFLECTION POINT DETECTION*

```
/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */

//package main;

import java.lang.*;
import java.io.*;
import java.util.*;

/**
 *
 * @author dbthaw
 */
public class main {

    /**
     * @param args the command line arguments
     *
     */


    public static void main(String[] args) {

        PRE5 pre = new PRE5();
        PUE5 pue = new PUE5();

        double pre_local_max = 0;
        double pue_local_max = 0;
        double pre_max = 0;
        double pue_max = 0;

        double pre_val = 0;
        double pue_val = 0;

        int t1_pre = 0;
        int t1_pue = 0;
        int t2_pre = 0;
        int t2_pue = 0;

        double t1_pre_val = 0;
        double t1_pue_val = 0;
        double t2_pre_val = 0;
        double t2_pue_val = 0;

        double[] puevals = new double[133];
        int[] pues = new int[133];

        double[] prevals = new double[133];
        int[] pres = new int[133];
        for (int i=1;i < 133;i++) {
            pre_val = pre.compute(i);
            if (pre_val > pre_max) {
                pre_max = pre_val;
                t2_pre = i;
            } // end if
            if ((pre_val > pre_local_max) && (i < 40)) pre_local_max =
pre_val;
            if ((pre_val > pre_local_max) && (i >= 40) && (t1_pre ==
0)) {
                t1_pre = i;
                t1_pre_val = pre_val;
            } // end if

            pue_val = pue.compute(i);
            if (pue_val > pue_max) {
                pue_max = pue_val;
                t2_pue = i;
            } // end if
            if ((pue_val > pue_local_max) && (i < 40)) pue_local_max =
pue_val;
            if ((pue_val > pue_local_max) && (i >= 40) && (t1_pue ==
0)) {
                t1_pue = i;
                t1_pue_val = pue_val;
            } // end of

            puevals[i] = pue_val;
            pues[i] = i;

            prevals[i] = pre_val;
            pres[i] = i;

        } // end for loop

        t2_pre_val = pre_max;
        t2_pue_val = pue_max;


        System.out.println();
        System.out.println("t1_pre: " + t1_pre + ", t1_pre_val: " +
t1_pre_val);
        System.out.println("t2_pre: " + t2_pre + ", t2_pre_val: " +
t2_pre_val);
        System.out.println();
        System.out.println("t1_pue: " + t1_pue + ", t1_pue_val: " +
t1_pue_val);
        System.out.println("t2_pue: " + t2_pue + ", t2_pue_val: " +
t2_pue_val);
        System.out.println();

        System.out.flush();
        /*File writeFile = new File("c:\\My
Documents\\+Classes\\+dissertation\\Data\\puevals.txt");
        PrintWriter out = null;
        try {
            out = new PrintWriter(writeFile);
        } catch (FileNotFoundException e) {
            e.printStackTrace();
        } // end try-catch


        out.print("dates,breaches\n");
        for (int i=1;i < 133;i++) {
            out.print(pues[i] + ",");
            out.print(puevals[i] + "\n");
        } // end for loop

        out.flush();

        writeFile = new File("c:\\My
Documents\\+Classes\\+dissertation\\Data\\prevals.txt");
        out = null;
        try {
            out = new PrintWriter(writeFile);
        } catch (FileNotFoundException e) {
            e.printStackTrace();
        } // end try-catch


        out.print("dates,breaches\n");
        for (int i=1;i < 133;i++) {
            out.print(pres[i] + ",");
            out.print(prevals[i] + "\n");
        } // end for loop

        out.flush();*/



        /*double testval = 0;

        try {
            testval = Double.parseDouble(args[0]);
        } catch (Exception e) {
            e.printStackTrace();
            System.exit(-1);
        } // end try-catch

        System.out.println();
        System.out.println("x = " + testval + ": " +
test.compute(testval));
        System.out.flush();*/


    } // end function main
} // end class main

class PRE5 {

    public double y;
    public double b;
    public double m1;
    public double m2;
    public double m3;
    public double m4;
    public double m5;
    //public double m6;

    public PRE5() {

        b = -2.405 * Math.pow(10, 0);
        m1 = 6.398 * Math.pow(10, -1);
        m2 = -3.748 * Math.pow(10, -2);
        m3 = 7.787 * Math.pow(10, -4);
        m4 = -6.118 * Math.pow(10, -6);
        m5 = 1.613 * Math.pow(10, -8);
        //m6 = 3.756 * Math.pow(10, -10);

        y = 0;

    } // end constructor

    public double compute(double x) {
        /*System.out.println("x^6 = " + Math.pow(x,6));
        System.out.println("x^5 = " + Math.pow(x,5));
        System.out.println("x^4 = " + Math.pow(x,4));
        System.out.println("x^3 = " + Math.pow(x,3));
        System.out.println("x^2 = " + Math.pow(x,2));
        System.out.println("x^1 = " + Math.pow(x,1));
        System.out.println();
        System.out.flush();*/

        //y = (m6 * Math.pow(x,6)) + (m5 * Math.pow(x,5)) + (m4 *
Math.pow(x,4)) + (m3 * Math.pow(x,3)) + (m2 * Math.pow(x,2)) + (m1 * x)
+ b;
        y = (m5 * Math.pow(x,5)) + (m4 * Math.pow(x,4)) + (m3 *
Math.pow(x,3)) + (m2 * Math.pow(x,2)) + (m1 * x) + b;
        /*System.out.println("y = " + y);
        System.out.flush();*/

        return y;

    } // end function compute

} // end class

class PUE5 {

    public double y;
    public double b;
    public double m1;
    public double m2;
    public double m3;
    public double m4;
    public double m5;
    /*public double m6;
    public double m7;
    public double m8;
    public double m9;*/

    public PUE5() {

        b = -2.969 * Math.pow(10,0);
        m1 = 9.419 * Math.pow(10,-1);
        m2 = -5.628 * Math.pow(10,-2);
        m3 = 1.180 * Math.pow(10,-3);
        m4 = -9.231 * Math.pow(10,-6);
        m5 = 2.383 * Math.pow(10,-8);
        /*m6 = -1.569 * Math.pow(10,-7);
        m7 = 1.260 * Math.pow(10,-9);
        m8 = -5.399 * Math.pow(10,-12);
        m9 = 9.585 * Math.pow(10,-15);*/

    } // end constructor

    public double compute(double x) {
        /*System.out.print("x^1 = " + Math.pow(x,1) + ", ");
        System.out.print("x^2 = " + Math.pow(x,2) + ", ");
        System.out.print("x^3 = " + Math.pow(x,3) + ", ");
        System.out.print("x^4 = " + Math.pow(x,4) + ", ");
        System.out.print("x^5 = " + Math.pow(x,5) + ", ");
        System.out.print("x^6 = " + Math.pow(x,6) + ", ");
        System.out.print("x^7 = " + Math.pow(x,7) + ", ");
        System.out.print("x^8 = " + Math.pow(x,8) + ", ");
        System.out.print("x^9 = " + Math.pow(x,9) + ", ");
        System.out.println();
        System.out.flush();*/

        //y = (m9 * Math.pow(x,9)) + (m8 * Math.pow(x,8)) + (m7 *
Math.pow(x,7)) + (m6 * Math.pow(x,6)) + (m5 * Math.pow(x,5)) + (m4 *
Math.pow(x,4)) + (m3 * Math.pow(x,3)) + (m2 * Math.pow(x,2)) + (m1 * x)
+ b;
        y = (m5 * Math.pow(x,5)) + (m4 * Math.pow(x,4)) + (m3 *
Math.pow(x,3)) + (m2 * Math.pow(x,2)) + (m1 * x) + b;

        /*System.out.println("y = " + y);
        System.out.flush();*/

        return y;

    } // end function compute


} // end class
```

6.15 Appendix D.2 – Java Code for Running Differential Averages (Method 3)

```
/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */


/**
 *
 * @author dbthaw
 */

import java.io.*;
import java.util.*;
import java.text.*;

public class main {

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) throws IOException {
        // TODO code application logic here

        /*File writeFile = new File("c:\\My
Documents\\+Classes\\+dissertation\\Data\\output.txt");
        PrintWriter out = null;
        try {
            out = new PrintWriter(writeFile);
        } catch (FileNotFoundException e) {
            e.printStackTrace();
        } // end try-catch*/

        /*String filename;
        FileReader inFileReader = null;
        BufferedReader in = null;

        filename = new String("dataloss_monthly.csv");

        try {
                inFileReader = new FileReader(filename);
                in = new BufferedReader(inFileReader);
        } catch (FileNotFoundException e) {
                System.out.println("Invalid input file: " + filename);
                System.exit(0);
        } catch (IOException e) {
                System.out.println("Unknown I/O error.");
                e.printStackTrace();
                System.exit(0);
        } // end try-catch*/

        File f = new File ("dataloss_monthly.csv");
        Scanner s = new Scanner(f);

        int num = 132; // Jan 2000 - Dec 2010

        int[] ids = new int[num];
        //SimpleDateFormat[] dates = new SimpleDateFormat[120];
        Date[] dates = new Date[num];
        int[] financeTotals = new int[num];
        int[] healthcareTotals = new int[num];
        int[] regulatedTotals = new int[num];
        int[] unregulatedTotals = new int[num];
        int[] totalBreaches = new int[num];
        int i = 0;

        //System.out.println(s.nextLine());

        while (s.hasNextLine()) {
            String line = s.nextLine();
            //System.out.println("line: " + line);
            StringTokenizer tokens = new StringTokenizer(line);
            int id = Integer.parseInt(tokens.nextToken(","));
            //SimpleDateFormat datecounter = new
SimpleDateFormat(tokens.nextToken().substring(1,11));
            String token = tokens.nextToken();
            //System.out.println("token: " + token);
            //int year = Integer.parseInt(token.substring(1,5));
            //System.out.println("year: " + year);
            //int month = Integer.parseInt(token.substring(6,8));
            //int day = Integer.parseInt(token.substring(9,11));
            //System.out.println("day: " + day);
            //System.out.println("parse: " + year + month + day);
            //Date datecounter = new Date(year, month, day);
            int financeTotal = Integer.parseInt(tokens.nextToken());
            int healthcareTotal = Integer.parseInt(tokens.nextToken());
            int regulatedTotal = Integer.parseInt(tokens.nextToken());
            int unregulatedTotal =
Integer.parseInt(tokens.nextToken());
            int total = Integer.parseInt(tokens.nextToken());

            ids[i] = id;
            //dates[i] = datecounter;
            financeTotals[i] = financeTotal;
            healthcareTotals[i] = healthcareTotal;
            regulatedTotals[i] = regulatedTotal;
            unregulatedTotals[i] = unregulatedTotal;
            totalBreaches[i] = total;


            i++;

        } // end while loop

        double maxDiff = -1;
        int maxDiffCounter = -1;
        double Ma_final = -1;
        double Mb_final = -1;
        double Mc_final = -1;
        double Md_final = -1;
        double diffReg_final = -1;
        double diffUnreg_final = -1;

        for (int j=2;j<i;j++) {
            int Sa = 0;
            int Sb = 0;
            int Sc = 0;
            int Sd = 0;

            for (int x=0;x < j;x++) {
                Sa += regulatedTotals[x];
                Sc += unregulatedTotals[x];
                //System.out.println("Sa: " + Sa);
                //System.out.println("Sc: " + Sc);
            } // end for loop
            for (int x=j;x < num;x++) {
                Sb += regulatedTotals[x];
                Sd += unregulatedTotals[x];
                //System.out.println("Sb: " + Sb);
                //System.out.println("Sd: " + Sd);
           } // end for loop

            double Ma = ((double)Sa / (double)j);
            double Mb = ((double)Sb / (double)(num - j));

            double Mc = ((double)Sc / (double)j);
            double Md = ((double)Sd / (double)(num - j));

            double diffReg = Mb - Ma;
            double diffUnreg = Md - Mc;

            /*System.out.println("Sa: " + Sa);
            System.out.println("j: " + j);
            System.out.println("Ma: " + Ma);
            System.out.println("Mb: " + Mb);
            System.out.println("Mc: " + Mc);
            System.out.println("Md: " + Md);*/

            if ((diffReg + diffUnreg) > maxDiff) {
                maxDiff = diffReg + diffUnreg;
                maxDiffCounter = j;
                Ma_final = Ma;
                Mb_final = Mb;
                Mc_final = Mc;
                Md_final = Md;
                diffReg_final = diffReg;
                diffUnreg_final = diffUnreg;


            } // end if
```

```
        } // end for loop

        double xa = (double)(maxDiffCounter / 2);
        double xb = (double)(((num - maxDiffCounter) / 2) +
maxDiffCounter);

        double Sr = ((Mb_final - Ma_final) / (xb - xa));
        double Su = ((Md_final - Mc_final) / (xb - xa));

        System.out.println("maxDiff: " + maxDiff);
        System.out.println("maxDiffCounter: " + maxDiffCounter);
        System.out.println("Ma_final: " + Ma_final);
        System.out.println("Mb_final: " + Mb_final);
        System.out.println("Mc_final: " + Mc_final);
        System.out.println("Md_final: " + Md_final);
        System.out.println("diffReg_final: " + diffReg_final);
        System.out.println("diffUnreg_final: " + diffUnreg_final);
        System.out.println();
        System.out.println("xa: " + xa);
        System.out.println("xb: " + xb);
        System.out.println("Sr: " + Sr);
        System.out.println("Su: " + Su);

        System.out.println("\nmaxDiffCounter: 72 --> 12/1/2005\n\nMa:
regulated avg. before t0\nMb: regulated avg. after t0\n\nMc:
unregulated avg. before t0\nMd: unregulated avg. after t0\n");


    }

}
```

6.16 Appendix E.1 – Tabular Comparison of NRC Report Information Security "Practice Areas" and CISSP Domains

CISSP Domain	Corresponding NRC Report "Practice Areas"
1. Access Control	Secure and Reliable Authentication Practices
2. Application Development Security	Incorporation of Security into System Design
3. Business Continuity and Disaster Recovery	*(none)*
4. Cryptography	Secure Information Exchange Among Public Principals
5. Information Security Governance and Risk Management	*(none)*
6. Legal, Regulations, Compliance and Investigations	*(none)*
7. Operations Security	Secure and Reliable Authentication Practices; Secure Information Exchange Among Public Principals; Automation of Intrusion Detection/Real-Time Analysis
8. Physical (Environmental) Security	*(none)*
9. Security Architecture and Design	Incorporation of Security Into System Design
10. Telecommunications and Network Security	*(none)*
(none)	Collaboration and Information Sharing

6.17 *APPENDIX F.1 – CHILDREN'S ONLINE PRIVACY PROTECTION ACT*

The Children's Online Privacy Protection Act (COPPA) provides that:[336]

> (b)(1) Not later than 1 year after October 21, 1998, the [Federal Trade] Commission shall promulgate under Section 553 of Title 5 regulations that:
>
> > (A) require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child [subsections omitted];
> >
> > (B) require the operator to provide, upon request of a parent under this subparagraph whose child has provided personal information to that website or online service, upon proper identification of that parent, to such parent [subsections omitted];
> >
> > (C) prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and
> >
> > (D) require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

[336] Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2581 (codified as amended at 15 U.S.C. §§ 6501-6506).

6.18 Appendix F.2 – HIPAA Definition of "Business Associate"

Business Associates are defined as:[337]

> (1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who:
>
> (i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:
>
> (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
>
> (B) Any other function or activity regulated by this subchapter; or
>
> (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
>
> (2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.
>
> (3) A covered entity may be a business associate of another covered entity.

[337] 45 C.F.R. § 160.103.

6.19 APPENDIX F.3 – FTC GLBA SAFEGUARDS RULE

The FTC’s GLBA Safeguards Rule specifies what each information security program shall contain, requiring that “in order to develop, implement, and maintain [a] information security program, [regulated organizations] shall: [338]

> (a) Designate an employee or employees to coordinate your information security program.
> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
>
> > (1) Employee training and management;
> > (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
> > (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
>
> (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
> (d) Oversee service providers, by:
>
> > (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
> > (2) Requiring your service providers by contract to implement and maintain such safeguards.
>
> (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

[338] 16 C.F.R. § 314.4.

6.20 APPENDIX F.4 – GLBA INTERAGENCY GUIDELINES

The GLBA Interagency Guidelines specify in detail what elements each regulated organization's information security program must contain and what goals those elements must achieve: [339]

> 1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:
>
> a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.
> b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;
> c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
> d. Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;
> e. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;
> f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;
> g. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and
> h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.
>
> 2. Train staff to implement the bank's information security program.
> 3. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by

[339] 12 C.F.R. § 30, App. B § (III)(C).

the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

4. Develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of customer information and consumer information in accordance with each of the requirements of this paragraph III.

6.21 APPENDIX F.5 – EXCERPTS OF FTC ORDER IN BJ'S WHOLESALE CLUB

The following are excerpts from the Federal Trade Commission's Decision and Order in *In the Matter of BJ's Wholesale Club*:[340]

I. IT IS ORDERED that Respondent . . . shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards 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 consumers, including:

> A. the designation of an employee or employees to coordinate and be accountable for the information security program.
>
> B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to:
>
> > (1) employee training and management;
> >
> > (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and
> >
> > (3) prevention, detection, and response to attacks, intrusions, or other systems failures.
>
> C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.
>
> D. the evaluation and adjustment of Respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II. IT IS FURTHER ORDERED that Respondent obtain an assessment and report (an "Assessment") from a qualified, objective, independent third-party professional, using

[340] *See* Decision and Order, *In the Matter of BJ's Wholesale Club, Inc.*, FTC File No. 042-3160 (Sept. 20, 2005) *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.

procedures and standards generally accepted in the profession, within one hundred and eighty (180) days after service of the order, and biennially thereafter for twenty (20) years after service of the order that:

> A. sets forth the specific administrative, technical, and physical safeguards that Respondent has implemented and maintained during the reporting period;
>
> B. explains 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 consumers;
>
> C. explains how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and
>
> D. certifies 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, for biennial reports, has so operated throughout the reporting period. Each Assessment shall be prepared by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the first Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of Respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection . . . within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

6.22 *Appendix F.6 – FTC Allegations in Reed Elsevier, Inc. and Seisint, Inc.*

Specifically, the Commission alleged that: [341]

> 10. Until at least mid-2005, respondents engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security to prevent unauthorized access to the sensitive consumer information stored in databases accessible using Accurint verification products ("Accurint databases"). In particular, respondents failed to establish or implement reasonable policies and procedures governing the creation and authentication of user credentials for authorized customers accessing Accurint databases. Among other things, respondents:
>
> > (a) failed to establish or enforce rules sufficient to make user credentials hard to guess. For example, respondents allowed Accurint customers to use the same word, including common dictionary words, as both the password and user ID, or a close variant of the user ID as the password;
> > (b) permitted the sharing of user credentials among a customer's multiple users, thus reducing likely detection of, and accountability for, unauthorized searches;
> > (c) failed to require periodic changes of user credentials, such as every 90 days, for customers with access to sensitive nonpublic information;
> > (d) failed to suspend user credentials after a certain number of unsuccessful log-in attempts;
> > (e) allowed customers to store their user credentials in a vulnerable format in cookies on their computers;
> > (f) failed to require customers to encrypt or otherwise protect credentials, search queries, and/or search results in transit between customer computers and respondents' websites;
> > (g) allowed customers to create new credentials without confirming that the new credentials were created by customers rather than identity thieves;
> > (h) did not adequately assess the vulnerability of the Accurint web application and computer network to commonly known or reasonably foreseeable attacks, such as "Cross-Site Scripting" attacks; and
> > (i) did not implement simple, low-cost, and readily available defenses to such attacks.

[341] *See* Complaint, *In the Matter of Reed Elsevier, Inc. and Seisint, Inc.*, FTC File No. 052-3904 at ¶ 10 (Mar. 27, 2008) *available at* http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf.

6.23 APPENDIX F.7 – MASS. DATA SECURITY STANDARDS

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH[342]

Section:
17.01: Purpose and Scope
17.02: Definitions
17.03: Duty to Protect and Standards for Protecting Personal Information
17.04: Computer System Security Requirements
17.05: Compliance Deadline

17.01 Purpose and Scope

(1) Purpose
This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

(2) Scope
The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

17.02: Definitions

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

Breach of security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information,

[342] 201 MASS. CODE REGS. 17.00.

maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

Personal information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account; provided, however, that “Personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

17.03: Duty to Protect and Standards for Protecting Personal Information

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information

security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

(a) Designating one or more employees to maintain the comprehensive information security program;

(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

1. ongoing employee (including temporary and contract employee) training;

2. employee compliance with policies and procedures; and

3. means for detecting and preventing security system failures.

(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information.

(f) Oversee service providers, by:

1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and

2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person’s behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

(g) Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.

(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

(i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: Computer System Security Requirements

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a

security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

(1) Secure user authentication protocols including:

(a) control of user IDs and other identifiers;

(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

(c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

(d) restricting access to active users and active user accounts only; and

(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(2) Secure access control measures that:

(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and

(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;

(5) Encryption of all personal information stored on laptops or other portable devices;

(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

17.05: Compliance Deadline

(1) Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

REGULATORY AUTHORITY
201 CMR 17.00: M.G.L. c. 93H

6.24 APPENDIX G.1 – CREATIVE COMMONS LICENSE

This is the text of Creative Commons' Attribution-NonCommercial-NoDerivs License, version 3.0.[343]

I. License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THEWORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED. BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

> (a) "Collective Work" means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with one or more other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.
>
> (b) "Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.

[343] *See* Attribution-NonCommercial-NoDerivs 3.0 United States, http://creativecommons.org/licenses/by-nc-nd/3.0/us/ (last visited Apr. 14, 2011).

(c) “Licensor” means the individual, individuals, entity or entities that offers the Work under the terms of this License.

(d) “Original Author” means the individual, individuals, entity or entities who created the Work.

(e) “Work” means the copyrightable work of authorship offered under the terms of this License.

(f) “You” means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

2. Fair Use Rights. Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

(a) to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works; and,

(b) to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works. The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats, but otherwise you have no rights to make Derivative Works. All rights not expressly granted by Licensor are hereby reserved, including but not limited to the rights set forth in Sections 4(d) and 4(e).

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

(a) You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of a recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this

License and to the disclaimer of warranties. When You distribute, publicly display, publicly perform, or publicly digitally perform the Work, You may not impose any technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any credit as required by Section 4(c), as requested.

(b) You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file-sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

(c) If You distribute, publicly display, publicly perform, or publicly digitally perform the Work (as defined in Section 1 above) or Collective Works (as defined in Section 1 above), You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or (ii) if the Original Author and/or Licensor designate another party or parties (e.g. a sponsor institute, publishing entity, journal) for attribution ("Attribution Parties") in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; the title of the Work if supplied; to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work. The credit required by this Section 4(c) may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear, if a credit for all contributing authors of the Collective Work appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this clause for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Author, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.

(d) For the avoidance of doubt, where the Work is a musical composition:

i. Performance Royalties Under Blanket Licenses. Licensor reserves the exclusive right to collect whether individually or, in the event that Licensor is a member of a performance rights society (e.g. ASCAP, BMI, SESAC), via that society, royalties for the public performance or public digital performance (e.g. webcast) of the Work if that performance is primarily intended for or directed toward commercial advantage or private monetary compensation.

ii. Mechanical Rights and Statutory Royalties. Licensor reserves the exclusive right to collect, whether individually or via a music rights agency or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work (“cover version”) and distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions), if Your distribution of such cover version is primarily intended for or directed toward commercial advantage or private monetary compensation.

(e) Webcasting Rights and Statutory Royalties. For the avoidance of doubt, where the Work is a sound recording, Licensor reserves the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions), if Your public digital performance is primarily intended for or directed toward commercial advantage or private monetary compensation.

5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND ONLY TO THE EXTENT OF ANY RIGHTS HELD IN THE LICENSED WORK BY THE LICENSOR. THE LICENSOR MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MARKETABILITY, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT AL- LOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR

EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

(a) This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collective Works (as defined in Section 1 above) from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

(b) Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

(a) Each time You distribute or publicly digitally perform the Work (as defined in Section 1 above) or a Collective Work (as defined in Section 1 above), the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

(b) If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

(c) No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

(d) This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor. Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, Creative Commons does not authorize the use by either party of the trademark “Creative Commons” or any related trademark or logo of Creative Commons without the prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons’ then current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time. For the avoidance of doubt, this trademark restriction does not form part of this License. Creative Commons may be contacted at http://creativecommons.org/.