DATA BREACH (REGULATORY) EFFECTS

David Thaw†

Breach notification laws have been a major driver of data protection efforts in U.S. organizations for more than a decade. This form of disclosure-based regulation exists in 47 of 50 U.S. states, as well as four other U.S. jurisdictions, but has yet to be adopted as a law of general applicability at the federal level.

This Essay considers the effects the structure of existing disclosure-based cybersecurity regulation has on the efficacy of U.S. firms' cybersecurity measures. Drawing on previous empirical work and analysis of firm incentives, it suggests two modest conclusions about the most efficacious legal structures: (1) that any disclosure-based regulation should be part of a broader cybersecurity regulatory framework and (2) that any risk-of-harm threshold triggering notification should bear a presumption in favor of notification. Based on these conclusions, I suggest a preliminary regulatory prescription for policymakers considering adoption or standardization of disclosure-based regulation in the data protection context.

---

† David Thaw is an Assistant Professor of Law and Information Sciences at the University of Pittsburgh and an Affiliated Fellow of the Information Society Project at Yale Law School.

The author thanks the Canada-U.S. Law Institute at Case Western University School of Law and the participants in the Institute's 2015 symposium for their feedback and thoughtful commentary on the scope of cybersecurity. The author also thanks Derek Bambauer, Andrea Matwyshyn, Paul Mazzucco, and Mark Paulding for their many years of input on the question of what constitutes cybersecurity.

This Essay is based in part on Testimony the author gave before the United States House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade on this subject matter on July 18, 2013, *available at* http://democrats.energycommerce.house.gov/index.php?q=hearing/hearing-on-reporting-data-breaches-is-federal-legislation-needed-to-protect-consumers-subcom. The author thanks the University of Connecticut School of Law and the Yale Law School Information Society Project for their support of that project. All ideas contained in the original testimony and this work are the sole product of the author unless otherwise indicated, and all errors are the sole responsibility of the author.

The author welcomes comments/feedback at dbthaw@pitt.edu.

TABLE OF CONTENTS

INTRODUCTION

This Essay considers the function and effects of data breach notification regulatory regimes from the perspective of cybersecurity.[1] While there are many concerns relevant to a data breach notification regulatory regime, the focus of this Essay is cybersecurity implications. In that regard, it considers regulatory structures that are likely to produce more effective cybersecurity outcomes.[2] The primary basis for this analysis is application of empirical evidence and analytical modeling. While this Essay does suggest a few modest policy outcomes, it is not a normative piece in this regard.

I. CONSIDERING "CYBERSECURITY'S" SCOPE

The term "cybersecurity" is a concept that has become something of a misnomer. This is, in part, one of the biggest challenges facing cybersecurity—these varying definitions require different, sometimes conflicting skill sets and assume different goals. For example, consumer information data breaches are one of the most socially prevalent aspects of cybersecurity. Perhaps equally prevalent, however, in the U.S. social consciousness are the activities of foreign state-sponsored malicious actors.

Understanding the "cybersecurity problem" and addressing issues such as data breaches first requires defining a rubric for considering

---

[1] *See infra* notes 5–6 (regarding use of the term "cybersecurity").

[2] Efficacy can be measured by a variety of metrics but, for the purposes of this Essay, "more effective at preventing system or data comprise" as a vague, general definition is sufficient to distinguish the focus of this work from other works. For further discussion of this topic, see generally David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 291–93, 294, 342–43 (2014) (discussing how "cybersecurity" efficacy might be empirically evaluated).

what are the units of analysis for entities we seek to protect and what are the substantive areas of expertise and practice which comprise "security."

This analysis begins with the latter question of what comprises security. While perhaps uncommon to consider the evaluative measure before considering the goal to be evaluated, the degree of ambiguity surrounding "cybersecurity" requires first discussing the term's meaning. By its own etymological roots, the word is misleading—the root "cyber" historically referred to "electronic system[s] of interlinked networks of computers . . . ."[3] The root first appeared in 1961 and has expanded in meaning to include later technologies—such as the Internet—but has always retained its core focus on computers and computing technologies.[4] Not all aspects of the security of computing and information systems, however, are technological in nature.

Using the term *cyber*security thus is potentially misleading—it implies a sole focus on technological defenses, when many "cybersecurity" compromises actually result from attack vectors primarily compromising a physical or administrative measure. Consider, for example, the means by which the Stuxnet malware is widely believed to have been delivered. The predominant theory is that it infected the control systems of target nuclear material enrichment facilities via a universal serial bus (USB) thumb drive carrying the malicious code.[5] While it is true that there exist technological protection measures to provide additional secondary defenses in the event a malicious USB drive is smuggled into a facility, a focus on these "technological" defenses both ignores the primary threat and is an inefficient use of resources. *Why was an unauthorized drive allowed into a sensitive area to begin with?* This is a question of *physical* security. Similarly, some questions surround the business processes by which an organization operates—are those processes, such as the identity verification questions asked by a call center operator,

---

3 WEBSTER'S NEW WORLD COLLEGE DICTIONARY 343 (3d ed. 1997).

4 OXFORD ENGLISH DICTIONARY, "cyber-, *comb. form*" (3d ed. Jan. 2009), *available at* http://www.oed.com/view/Entry/250879?rskey=yfQWME&result=7#.

5 *See, e.g.*, Pete Pachal, *U.S. Launched Its Biggest Cyberattack From a Thumb Drive*, MASHABLE (June 1, 2012), http://mashable.com/2012/06/01/stuxnet-thumb-drive; Joshua Kopstein, *Stuxnet Virus Was Planted by Israeli Agents Using USB Sticks, According to New Report*, THE VERGE (Apr. 12, 2012, 7:32 PM), http://www.theverge.com/2012/4/12/2944329/stuxnet-computer-virus-planted-israeli-agent-iran. A Google search of "how was Stuxnet delivered," demonstrates that the majority of media articles on the topic overwhelmingly support the position that delivery was via a physically-inserted USB drive, notwithstanding a few positions to the contrary asserting a network payload delivery mechanism. Those alternative positions appear to be contradicted by further evidence that the malware "spread" upon which they base their claim was in fact a result of unintentional containment failure after infection resulting from programming errors by the malware developers, not as the result of a sophisticated technical attack as some sources presume. GOOGLE, https://www.google.com (search "how was Stuxnet delivered;" then follow the hyperlinks for the media articles on the first page) (last visited Apr. 24, 2015).

vulnerable to attack? These are questions of *administrative* security.

These examples describe two areas of security ("physical" and "administrative") that are distinct from "technological" security. Collectively, these three elements adequately describe the aspects of security.[6] Many existing legal frameworks recognize this typology.[7] Thus, as I and others describe elsewhere, the concept of "information security" more accurately describes the exercise of data and information system protection.[8]

Thus, when considering cybersecurity, a holistic evaluation, including the full range of aspects described above, is critical. Nonetheless, while the term "information security" therefore is more descriptive, this Essay adopts the term "cybersecurity" for consistency with popular writing on the subject.[9]

Against what, then, do our laws and regulations seek to protect? Scholars, public commentators, and policymakers include a vast array of systems in discussion of what "cybersecurity" seeks to protect. While in some contexts, such as privacy, this ambiguity may have advantages, in the more objective context of security[10] ambiguity may lead to misapplication of techniques and mismatch between security measures

---

6 Social, economic, and other related factors are orthogonal to this typology—for example, a psychological (e.g., social engineering) attack may take place against a business process (e.g., the call center) or against a technical system (e.g., an email "phishing" attack).

7 *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (relevant portions codified at 42 U.S.C. § 1320d-2(d)(2), implementing regulations codified at 45 C.F.R. § 164); Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (relevant portions codified at 15 U.S.C. § 6801(b), implementing regulations codified at 16 C.F.R. § 314); MASS. GEN. LAWS ch. 93H, § 2 (2015) (implementing regulations codified at 201 MASS. CODE REGS. 17.01–.05). *See also generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

8 As noted by Professor Andrea Matwyshyn, "[r]eferring to all of information security, particularly in private sector contexts, as 'cybersecurity' is technically incorrect." Matwyshyn describes this misnomer as ignoring the aspects of physical security inherent in "holistic" protection of data maintained by an enterprise. I concur with this assessment, and further suggest, as consistent with the administrative/technical/physical breakdown adopted by the health care cybersecurity example (42 U.S.C. § 1320d-2(d)(2)), that such a characterization also overlooks the administrative aspects involved in protecting security information. *See* Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NW. U. L. REV. 795, 817, n.99 (2013); *see also* David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907 (2013) (discussing the distinction between purely technical restrictions on computer usage and comprehensive administrative, technical, and physical restrictions thereon). Cybersecurity remains the common term with which most readers will be familiar, and thus I utilize that term when describing the matter generally. I further discuss this distinction in later work. *See generally* David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 331 n.2 (2014) [hereinafter Thaw, *Enlightened Regulatory Capture*] (discussing when usage of the term "information security" may be appropriate even when the term "cybersecurity" is adopted for the purposes of literary consistency).

9 *See* Thaw, *Enlightened Regulatory Capture*, *supra* note 8, at 331 n.2.

10 *See generally* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667 (2013).

and protection goals. For example, the security techniques and goals for protection of strategic weapon control systems are different than the techniques and goals for an average consumer, for example, protecting their personal computer used primarily for entertainment purposes.

Defining the unit of analysis that a cybersecurity law or regulation seeks to address is critical. Approaches necessary for military environments may be ill-suited—or possibly even damaging—to ordinary consumer-based commercial environments. This Essay proposes a four-part classification for entities:

> (1) *Military, intelligence, and other high-reliability or sensitive government operations*[11];
>
> (2) *Privately operated "critical infrastructure,"* utilities, communications networks, and other infrastructure operated by private entities but requiring high-reliability operations or utilizing meaningful sensitive information;
>
> (3) *Public and other government operations*, which are not otherwise sensitive or high-reliability;
>
> (4) *Non-critical/non-sensitive private entities*, private entities that neither require high-reliability operations nor utilize meaningful amounts of sensitive information.

These four categories operate generally along a spectrum from lowest risk-tolerance (category 1) to highest risk-tolerance (category 4). Risk-tolerance is not necessarily linear in this regard, however, and primarily comprises two metrics: (1) "risk-tolerance," the degree of sensitivity of information involved in operations and the degree of reliability[12] required for operations, and (2) "efficiency requirements," the degree of operational efficiency impairment that an entity can absorb, while continuing to provide its primary function, operation, good, or service. With these two metrics, the four categories comprise a two-by-two matrix more appropriate for analysis:

---

[11] Law enforcement activities split across categories 1 and 3. Quite obviously, certain activities such as anti-terrorism, counter-intelligence operations, RICO, and other undercover operations would fall under category 1. Other operations such as civil enforcement (e.g., parking) and community policing efforts seem well-aligned with category 3. Some activities pose grey areas on which law enforcement experts are likely to disagree. Such disagreement, and indeed the idea that law enforcement splits across these categories, however, is outside the scope of and not relevant to the conclusions of this Essay.

[12] *See* Bambauer, *supra* note 10.

	High-Efficiency Requirements	Reduced Efficiency Requirements
Limited Risk-Tolerance	• **Government: Critical** *(Category 1)*	• **Government: Non-Critical** *(Category 3)*
Greater Risk-Tolerance	• **Private: Critical Infrastructure*** *(Category 2)*	• **Private: Non-Critical** *(Category 4)*

** While certain aspects of privately operated critical infrastructure have lower risk-tolerance than others (e.g., electrical and water grids), such infrastructure overwhelmingly is provided by for-profit private entities.*[13]

A more extensive discussion of this typology is forthcoming in *Cybersecurity Stovepiping*;[14] however, for the purposes of this analysis of data breach regulation, the "risk tolerance" axis is informative. The substantial majority of jurisdictions' breach notification statutes do not apply to government entities.[15] For this reason, the analysis in this Essay focuses on the implications for private entities. Private entities vary in their "efficiency requirements" but generally have a greater risk-tolerance, as they primarily comprise for-profit enterprises that have a primary fiduciary responsibility to deliver financial return to their shareholders/owners. If the cost of the required degree of security for satisfactory operation were to exceed the ability of such organizations to provide a good or service, the standard market expectation would be that the organization would discontinue provision of the good or service—not that they would incur a loss by doing so.

For these reasons, private entities must be considered as a separate unit of analysis for the purpose of considering the effects of data breach regulation. The remaining Parts assume private entities as the unit of analysis and do not differentiate between private "critical infrastructure" (category 2) and "non-critical" private entities (category 4), as the points made in those Parts are equally applicable to both categories.

---

[13] For a more thorough analysis, see Thaw, *infra* note 14.

[14] David Thaw, *Cybersecurity Stovepiping* (Univ. of Pitt. Sch. of Law Legal Studies Research Paper, forthcoming 2016), *available at* http://ssrn.com/abstract=2572012.

[15] *See generally*, *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGIS., http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Apr. 5, 2015) (providing direct links to a multi-jurisdictional survey of the data breach notification laws in place as of the time of this writing, excluding federal industry sector-specific statutes/regulations).

II. COMPREHENSIVE REGULATORY FRAMEWORKS

Legislatures often consider data breach notification regulation distinctly from other elements of cybersecurity regulation. Of the 51 U.S. jurisdictions to have adopted such regulations, nearly all (except Massachusetts) did so originally as a free-standing statute, and only a few additional jurisdictions (e.g., California, Nevada) have later amended their regulations to expand the scope beyond breach notification.[16]

This Essay proposes two reasons why breach notification should not continue to be adopted in this standalone, piecemeal fashion. First, doing so creates the risk of unanticipated consequences and "definitional lock-in." Second, empirical research demonstrates that comprehensive cybersecurity regulation is nearly four times more effective at preventing reportable breaches than are breach notification regulations alone.

A. *"Definitional Lock-In": The Risks of Standalone Breach Notification*

Standalone regulation is attractive to legislatures. It reduces technical complexity, eases the burden of legislative drafting, and may be more politically feasible than comprehensive approaches. Piecemeal regulation, however, ignores the general concern that when later regulations must be adopted, such adoption does not occur in a vacuum—and may interact in unexpected ways with previous regulations.[17] Breach notification should be considered as part of overall, comprehensive cybersecurity regulation to avoid unexpected results from such piecemeal approaches.

Adopting standards for breach notification in the absence of comprehensive cybersecurity regulation will create "definitional lock-in" for categories defined to serve the purpose of breach notification but not well-suited for later adoption to broader, comprehensive cybersecurity regulation. Key definitions in regulations will be determined at an early stage, based on a limited scope of purpose not well-suited for the broader purposes later envisioned. Specifically, key definitions, such as the subject of information to be protected (often referred to as "Personal Information"), will be defined for the purposes of consumer breach notification. These purposes are likely very

---

16 *See* MASS. GEN. LAWS ch. 93H, §§ 2–3 (2015); CAL. CIV. CODE §§ 1798.29, 1798.81.5–1798.82 (West 2015); NEV. REV. STAT. §§ 603A.010 *et seq.* (2014).

17 Some scholars have indirectly suggested similar thoughts in other contexts. *See, e.g.*, Todd Donnelly Batson, Note, *No Vacancy: Why Immigrant Housing Ordinances Violate FHA and Section 1981*, 74 BROOK. L. REV. 131, 135 (2008).

different than those appropriate to comprehensive cybersecurity regulation. Lock-in occurs as a result of the substantial cost to organizations of later "re-classifying" information based on additional categories established by new regulation. This process, when applied to existing data,[18] is often cost-prohibitive and may raise regulatory burdens too high for effective compliance, thus pressuring legislators and regulators to retain existing definitions.

To be specific, consider the example of the types of information that should be subject to protection. In the case of breach notification, this information is most commonly referred to as "personal information" or "personally identifiable information." These terms have widely varying definitions. At the state level, a least common denominator exists: the combinations of an identifying item, most commonly an individual's name, with one of three categories of more sensitive information:

- the individual's Social Security Number;
- the individual's financial account numbers, along with any identification code necessary to access the account; or
- the individual's government-issued identification number (usually a driver's license or state identification).

The stated purpose of most jurisdictions' breach notification statutes is to enable consumers to take steps to protect themselves by requiring custodians of this information to inform consumers when those custodians have lost control of this information.[19] Yet many other types of information may pose a great harm to consumers. For example:

- medical records;
- wills;
- diaries;
- private correspondence (including e-mail);
- financial records;
- photographs of a sensitive or private nature; and
- similar information

are all categories of information federal criminal law considers sufficient to warrant substantial criminal sentence enhancements for individuals convicted of computer crimes involving identity theft.[20] The

---

18 As differentiated from new data generated as technology advances.

19 *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).

20 *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(16). *See also id.* at § 2B1.1 Application Notes.

Department of Health and Human Services,[21] the Department of the Treasury,[22] and the Federal Trade Commission[23] each have offered additional definitions of information they consider to be "sensitive" to consumers. All of this information should be the subject of consumer protection. Additionally, consumers should be informed whenever this information is subject to unauthorized disclosure as is necessary to take steps to protect themselves.

These categories are hardly comprehensive of the types of information that need to be protected by comprehensive cybersecurity regulations. Corporate trade secrets, including sensitive data about products not yet available outside the United States; sensitive business development plans; information about critical infrastructure systems, such as water, electric, or telecommunications grids; and cybersecurity plans are all sensitive information that are not the province of the general consumer. Yet a failure to secure this information may have costly effects, and not just to the organization experiencing the breach. If a business partner of a new pharmaceutical company fails properly to secure its information systems or the information technology services provider to a major financial institution or exchange fails to implement appropriate controls on administrative accounts, substantial negative effects to the broad economy may result if those systems are compromised. None of these eventualities necessarily involves consumer information, but each clearly demonstrates a public interest in collective security.

If a definition of information to be protected is developed based solely on consumer breach notification, the downstream cybersecurity implications will be costly. Either organizations must engage in expensive reclassification of information and redesign of their cybersecurity programs when new regulations are subsequently implemented, or large areas of information may be left vulnerable if the regulations fail to expand the definition of information to be protected. In either case, the cost of considering breach notification separate from comprehensive cybersecurity measures would be high.

---

21 See 45 C.F.R. § 160.103 for definition of "individually identifiable health information."

22 *See* 12 C.F.R. Pt. 364, App. B(I)(C)(2)(b) ("Consumer information means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the bank for a business purpose. Consumer information also means a compilation of such records. The term does not include any record that does not identify an individual.").

23 *See generally* Protecting Personal Information: A Guide for Business, FEDERAL TRADE COMM'N at 5, *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf (suggesting a broad definition of personal information that includes "other sensitive data").

B. *Comparative Efficacy: Comprehensive Regulation is More Effective*

In prior work, I examined the efficacy of existing cybersecurity regulations,[24] specifically including the breach notification statutes present in most U.S. jurisdictions, and compared the effectiveness of breach notification statutes and comprehensive cybersecurity regimes. I combined qualitative, semi-structured interviews of Chief Information Security Officers (CISO) at key U.S. organizations with quantitative analysis of data breach incidence from 2000 through 2010. The results described the effects of each regime at driving cybersecurity practices within organizations, based primarily on the CISO interviews.

The interviewees reported that a primary effect of breach notification laws was to focus intensive effort on encryption of portable devices and media containing personal information.[25] While effective at reducing the number of reportable breaches, some respondents reported that this resulted in focusing *too* much on only one area of security[26]—effectively leaving other venues vulnerable to attack. These attacks affect not only potential compromise of personal information as defined in existing breach notification statutes, but also the ability of outside attackers to compromise the integrity of critical infrastructure systems.

Such attacks are not hypothetical—in 1983, for example, a hacker group compromised the security of Memorial Sloan-Kettering Cancer Center in New York and gained access that effectively would have allowed them to alter the radiation treatment protocols of patients.[27] This compromise led to the addition in 1986 of a felony enhancement to the Computer Fraud and Abuse Act for damaging computer systems relating to medical care.[28]

As noted by the CISOs interviewed from the health care sector, breach notification statutes forced them to focus increased resources on encryption—without receiving additional resources to maintain existing programs.[29] The resultant reallocation of security budgets directed resources away from the areas those CISOs believed were most in need.[30] I describe this phenomenon as "Locking the Bank or Vault Door and Leaving the Back Window Open."[31] Focusing *solely* on consumer breach notification may have detrimental effects to other, critical areas of information security.

---

24 *See generally* Thaw, *supra* note 2.
25 *Id.* at 317–322.
26 *Id.*
27 *See* S. REP. NO. 99-432, at *2–3, 12 (1986).
28 *See id.*; *see also* 18 U.S.C. §§ 1030(a)(5), (c)(4)(A)(i)(II) (2012).
29 *See* Thaw, *supra* note 2, at 368.
30 *Id.*
31 *Id.* at 361.

The quantitative analysis conducted as part of this project confirms the comparative efficacy of comprehensive cybersecurity regulation. By analyzing periodic breach incidence data from January 1, 2000, through December 31, 2010, I determined that the combination of consumer breach notification and comprehensive cybersecurity regulation was as much as four times more effective at preventing reportable breaches of consumers' personal information than was breach notification alone.[32]

Piecemeal regulation certainly has political and practical advantages. Likewise, standalone breach notification regulation does have certain advantages, most notably including highlighting the presence of cybersecurity concerns by requiring organizations to report certain breaches of security.[33] However, these advantages are substantially outweighed by the risks of unanticipated consequences and definitional lock-in. When these risks are considered together with the comparative efficacy of preventing reportable breaches, a comprehensive approach to cybersecurity regulation is clearly appropriate.

III. AFFIRMATIVE PRESUMPTION FAVORING INVESTIGATION

The conclusions in Part II do not, of course, suggest that breach notification should be ignored. Quite the contrary—it is an essential component of a comprehensive cybersecurity regulatory framework. In considering the structure of this framework, however, it is crucial to examine the incentives created by various presumptions within the possible regulatory approaches. Any legal presumptions should favor incentives that encourage better security practices, such as the conduct of more thorough post-incident investigations.

When considering the issue of consumer breach notification, legislators and regulators frequently confront the issue of *when* to require notification. Among existing law, some jurisdictions require notification in all cases of loss-of-control (subject to the "encryption exception"[34]), whereas others adopt what is known as a "risk-of-harm" threshold.[35] The empirical data on the comparative efficacy of strict liability versus "risk-of-harm" notification thresholds is incomplete.[36]

---

[32] *Id.* at 355.

[33] *Id.* at 349, 371.

[34] See generally *Data Breach Charts*, BAKERHOSTETLER (2014), *available at* http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf for a 50-state survey.

[35] *Id.*

[36] As of the time of this writing, the author is unaware of any unclassified examination of this question. Some analyses have considered related questions but focus on other questions and are not informative as to this point. *See, e.g.*, Thaw, *supra* note 2. *See also, e.g.*, Sasha Romanosky, Rahul Telang, & Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30(2) J. POL'Y ANALYSIS & MGMT. 256 (2011); Sasha Romanosky, David A. Hoffman, &

The focus of this Part, therefore, addresses the cybersecurity implications of certain formulations of the risk-of-harm threshold. Specifically, for those jurisdictions adopting such a threshold, it is important to recognize that some formulations of the threshold negatively impact cybersecurity procedures and outcomes.

Risk-of-harm thresholds may have many forms but generally can be categorized according to the *affirmative* or *negative* presumption of notification. An *affirmative* presumption of notification requires a data custodian who experiences a breach to affirmatively demonstrate that the specified risk of harm threshold *is not satisfied* before they are exempted from consumer notification requirements. A *negative* presumption of notification *does not* require a data custodian who experiences a breach to notify consumers *unless* an investigation reveals that the specified risk of harm threshold has been satisfied.

A negative presumption of notification carries substantial, worrisome implications for cybersecurity procedures and outcomes. Specifically, this presumption disincentivizes organizations from conducting thorough security investigations.

Organizations have incentives to limit the scope and scale of investigations that may uncover information potentially exposing the organization to liability. For example, when conducting comprehensive cybersecurity assessments, auditing and consulting firms often work together with law firms so that the results of these assessments will be privileged as attorney-client work product and thus not subject to discovery in civil litigation or regulatory investigations. Clients of such firms often desire to learn about the risks they face, but do not want to incur liability for failure to remediate security vulnerabilities identified in the assessment. This problem is particularly compounded when faced with low-probability/high-risk vulnerabilities for which the cost of remediation is high. While generally protected by the business judgment rule, executives of publicly traded organizations still bear a fiduciary duty to act in the best interests of their shareholders. A risk analysis might well reveal that the probability is sufficiently low not to justify the direct costs of remediation when combined with the cost of business disruption and other indirect cost. While I do not suggest that organizations engage in willful ignorance of their legal or regulatory obligations, my research data and professional experience support the conclusion that organizations can have substantial incentive not to pursue a comprehensive investigation if it might trigger additional regulatory compliance requirements.[37] Conversely, if pursuing that investigation might alleviate the organization of regulatory compliance requirements (e.g., exempt the organization from consumer

Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74 (2014), *available at* http://ssrn.com/abstract=1986461.

[37] *See generally* Thaw, *supra* note 2.

notification), my research and professional experience support the conclusion that organizations can have substantial incentive to thoroughly pursue that investigation.

Thus, an *affirmative* presumption of notification is superior from a cybersecurity perspective. Such a presumption avoids disincentivizing thorough cybersecurity investigations, which are one of the most important tools in protecting consumers against future data breaches and securing existing information systems.

CONCLUSION

The primary goal of this Essay is to apply existing empirical analysis and analytical modeling to describe characteristics and suggest predictions about the function and effects of data breach notification laws. It suggests three primary conclusions in this regard. First, that a well-defined definition of cybersecurity, including the unit of analysis of protection, is critical to any discussion of data breach notification regulation. Second, that data breach notification regulation is more appropriate as part of a comprehensive cybersecurity regulatory regime. Third, that when using a risk-of-harm threshold for when notification is required, that threshold should employ an affirmative presumption requiring notification.

Notwithstanding this primary goal, these conclusions suggest some modest policy prescriptions. These suggestions build on similar regimes found in states such as New York,[38] Massachusetts,[39] and Virginia,[40] each of which require notification to central state regulatory authorities in addition to notification to consumers in the event of a reportable data breach. Such a bifurcated notification regime could be adopted at a federal level and in other nations currently without data breach notification regulations.

Under such a bifurcated notification regime, organizations experiencing a loss-of-control of any covered data would be required to report that incident to a centralized reporting authority, most likely a federal regulator such as the United States Federal Trade Commission. Consumer reporting would be triggered in certain cases deemed appropriate to when consumers can take steps to protect themselves and/or when consumers have an interest in awareness that their sensitive information was subject to unauthorized disclosure.

This bifurcated notification regime, if properly implemented, could achieve many of the goals of consumer breach notification while mitigating the risks of "over-notification" often raised by critics of strict

---

38 *See generally* N.Y. GEN. BUS. LAW § 899-aa (McKinney 2013).

39 *See generally* MASS. GEN. LAWS ch. 93H-1 (2015).

40 *See generally* VA. CODE ANN. § 18.2-186.6 (2014).

loss-of-control regimes.[41] Specifically, consumers would receive appropriate notification, while all incidents would nonetheless be reported. Thorough information security investigations would be a requirement under this regime as part of the centralized reporting requirement. Additionally, the regulatory agency receiving the reports would have the ability to follow up in cases where they suspect consumer notification should have occurred but did not, to follow up if there is evidence a broader pattern of information security deficiencies may be present, or to follow up and provide support if it believes the organization requires additional information security and/or law enforcement support.

I stress that this proposal is *preliminary*, and I lay out the basic characteristics as guidelines.

---

[41] This is not to suggest that valid empirical evidence exists indicating over-notification currently is or is not a problem. The conclusion, rather, only suggests that *if* over-notification is of concern (as suggested by some experts testifying before Congress), a bifurcated notification regime can address such concerns. *See, e.g.*, *Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the Comm. on House Energy & Commerce*, 113th Cong. 6 (July 18, 2013) (statement of Dan Liutikas, Chief Legal Officer, CompTIA), *available at* http://docs.house.gov/meetings/IF/IF17/20130718/101152/HHRG-113-IF17-Wstate-LiutikasD-20130718.pdf. *See also Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the Comm. on House Energy & Commerce*, 113th Cong. 9 (July 18, 2013) (statement of Jeffrey E. Greene, Senior Policy Counsel, Cybersecurity and Identity Symantec Corp.), *available at* http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Greene-CMT-Data-Breaches-Consumer-Protection-2013-7-18.pdf; *Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the Comm. on House Energy & Commerce*, 113th Cong. 6 (July 18, 2013) (statement of Kevin M. Richards, Senior Vice President, Federal Government Affairs TechAmerica), *available at* http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Richards-CMT-Data-Breaches-Consumer-Protection-2013-7-18.pdf. *See also generally Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the Comm. on House Energy & Commerce*, 113th Cong. (July 18, 2013) (Hearing Video Transcript), *available at* https://www.youtube.com/watch?feature=player_embedded&v=wk75dSAb8A8.