Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation

Andrea M. Matwyshyn†

ABSTRACT:

This article undertakes a normative and empirical legal inquiry into the manner in which information security vulnerabilities are being addressed through law and in the marketplace. Specifically, this article questions the current legislative paradigm for information security regulation by presenting a critique grounded in information security and cryptography theory. Consequently, this article advocates shifting our regulatory approach to a process-based security paradigm that focuses on improving the security of our system as a whole. Finally, this article argues that in order to accomplish this shift with the least disruption to current legal and economic processes, expanding an existing set of well-functioning legal structures is preferable to crafting new legal structures. Securities disclosure law is already focused on regulating the most connected points in our economy, publicly traded entities. Public companies provide a good starting point for spreading better information security behaviors because of this connectedness. As such, disclosure of public companies' information security behaviors will assist them in maximizing shareholder value and will assist regulators in finding the inadequately secure points in our economy.

TABLE OF CONTENTS

†Assistant Professor of Law/Executive Director, Center for Information Research, University of Florida; Affiliate, Centre for Economics and Policy, University of Cambridge. The author invites comments at matwyshyn@law.ufl.edu and wishes to thank Martin H. Redish, Cem Paya, Sharon M. Gordon, Charlotte Crane, Ronald J. Allen, James Lindgren, David Reuter, Marshall Shapo, Emerson Tiller, Andrea Monroe, Fred McChesney, Anthony D'Amato, Matthew Sag, Jennifer Hill, and Miluska Novota for their discussions with me on the subject matter of this article, their insightful commentary and their critiques. Special thanks to Jason Soncini for his excellent and indispensable research assistance.

Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation

Andrea M. Matwyshyn

INTRODUCTION

Our society currently sits at an information control crossroads. Advances in information technology have fundamentally altered the business environment[1] and created a marketplace suffering from a data control paradox: on one hand, aggregation and commercial leveraging of data is easier than ever before; on the other hand, protecting proprietary information is becoming increasingly difficult.[2] This data control paradox impacts both corporate entities and consumers. Personally identifiable information can simultaneously be conceptualized as both an individual consumer's information property[3] and, if collected with consent of the consumer, an entity's intangible asset which can be sold in the marketplace. Consequently, the issues raised by information security cut across all levels of social ecology.

Within the last five years, Congress has passed numerous data control statutes, including the Children's Online Privacy Protection Act,[4] the Gramm-Leach-Bliley Act,[5] the Health Insurance Portability and Accountability Act,[6]

---

1. For a discussion of the manner in which new technologies have fundamentally transformed traditional business processes, see, for example, Carolita Oliveros, *Overview of Global Internet Distribution Laws*, SJ075 ALI-ABA 579 (American Law Institute—American Bar Association Continuing Legal Education, 2004) (discussing international product distribution and marketing transformation in business as a result of the Internet).

2. For example, by the end of the first quarter of 2005, at least two major data control failures had occurred—the compromise of as many as 170,000 consumers' data by data aggregators ChoicePoint, Inc. and LexisNexis, as well as the loss of tapes with 1.2 million federal employees' information by Bank of America. *See* Associated Press, *Choicepoint Says It's Sorry*, WIRED NEWS, Mar. 15, 2005, http://www.wired.com/news/privacy/0,1848,66912,00.html?tw=wn_tophead_3; Kim Zetter, *California Woman Sues ChoicePoint*, WIRED NEWS, Feb. 24, 2005, http://www.wired.com/news/privacy/0,1848,66710,00.html?tw=wn_tophead_3; Kim Zetter, *ID Theft Victims Could Lose Twice*, WIRED NEWS, Feb. 23, 2005, http://www.wired.com/news/privacy/0,66685-1.html?tw=wn_story_page_next1. For a discussion of the Bank of America incident, see Paul Newell, *Bank of America Says Tapes with Customer Data Lost*, TECH. REV., Feb. 28, 2005, http://wwwnl.technologyreview.com/t?ctl=BE60DD:2EDABCF.

3. For a discussion of the transformation of user data into a marketable commodity and the appropriateness of intellectual property or tort remedies, see Jessica Litman, *Information Privacy/Information Property*, 52 STAN L. REV. 1283 (2000).

4. 15 U.S.C. §§ 6501-6506 (2004). COPPA applies to websites or online services that are operated for commercial purposes. *Id.* § 6501(2).

5. *Id.* §§ 6821-6827 (2004). GLBA governs the privacy protections for the customer information of financial institutions.

6. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (privacy provisions codified at 42 U.S.C. § 1320d-1320d-8 (2004)). HIPAA governs health information held by health plans, health care clearinghouses, or health care providers who transmit any health information in electronic form in connection with a

and the Controlling the Assault of Non-Solicited Pornography and Marketing Act.[7] Through these statutes, Congress has articulated a clear social directive to business entities to improve information security. Despite this Congressional action, however, information vulnerability[8] is reaching crisis levels within our society, bringing with it high long-run social costs.[9]

Both corporate entities and consumers have contributed to widespread information vulnerability. This article focuses on the first of these two sources, corporate entities,[10] and undertakes a normative and empirical legal inquiry into the manner in which information security vulnerability is being addressed through law and the marketplace. Specifically, this article questions the current legislative paradigm for information security regulation by presenting a critique grounded in information security and cryptography theory. This article next questions whether a correction to the current legal paradigm is necessary, or whether market forces are correcting for the legislative deficiency. It analyzes current industry practices of information security risk management by conducting an empirical analysis of the information security disclosure practices of publicly traded companies. Results of these analyses indicate that business entities, like Congress, have adopted the suboptimal security paradigm known as "security through obscurity." These results cast doubt on whether information risk is being incorporated into corporate and shareholder decision-making and whether information security learning is emerging in our society.

Consequently, this article advocates shifting our regulatory approach from a "security through obscurity" paradigm to a process-based security paradigm that focuses on improving the security of our system as a whole while facilitating entities' information security learning. In order to accomplish this

---

covered transaction.

7. CAN-SPAM is the acronym commonly used for the Controlling the Assault of Non-Solicited Pornography and Marketing Act. Pub. L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C. §§ 7701-7713 (2004)).

8. As used in this article, information or security vulnerability refers to any deficiency in security which may result in an online or offline breach or unauthorized access of data, including any use of corporate or consumer computer systems for malicious activity by internal or external forces and any related event, malicious or accidental, which results in damages or losses to a company or consumer such as a virus or worm.

9. One visible manifestation of this widespread vulnerability is the current epidemic of phishing attacks which simultaneously damage the corporate goodwill of the entities impersonated as well as the interests of consumers through the theft of their personally identifiable information. Simply put, phishing is luring a user to a replica of an existing website to trick a user into submitting personal, financial, or password data. *See* Anti-Phishing Working Group, http://www.antiphishing.org (last visited Nov. 23, 2004); WordSpy, http://www.wordspy.com/words/phishing.asp (last visited Nov. 23, 2004).

10. The focus of this article is on corporate education and development as to information security. Improving the state of corporate information security will generate a more potent effect in diminishing information crime. Corporations are aggregators of consumer data, thus creating the potential for many consumers to be harmed at once in a given data breach. Similarly, corporations are investments of many shareholders and thus the damage resulting from a breach of information security financially impacts shareholders as well as the entity. Consumer education is a critical part of improving information security but will take a longer period of time than improving the security of business entities.

shift with the least disruption to current processes, expanding an existing set of well-functioning structures is preferable to crafting new legal structures. Specifically, securities disclosure regulation is already focused on regulating the most connected points in our economy: publicly traded entities. Therefore, public companies provide a good starting point for spreading better information security behaviors through the economy.

Part I of this article introduces the information security crisis faced by business entities and consumers. Part I also discusses current legislative approaches to raise social and corporate awareness of the importance of information security. In the last ten years, Congress has articulated a new social policy directive to corporate entities to improve information security.

Part II examines how this directive is being incorporated into the economy. This part argues that the paradigm adopted by current information security regulation is suboptimal. Known in information security and cryptography theory as "security through obscurity," this paradigm is considered inferior to a security paradigm predicated on Kerckhoff's Law, or "security through process." Consequently, Part II advocates legislatively shifting toward a "security through process" paradigm in which the security of information throughout the economy must be analyzed as a whole, looking for the weakest points of security, and focusing on raising the average level of security throughout the system.

Part II also conducts an inquiry into the information security behaviors of the "hubs" in our economy, publicly traded entities, to analyze whether, despite the implementation of a suboptimal legislative paradigm, the information security behavior of such hub entities nevertheless evidences the paradigm of "security through process." If hubs are already incorporating a "security through process" paradigm, then regardless of the legislative approach, security learning may be spreading through our economy and perhaps legislative correction is unnecessary. An empirical longitudinal analysis of one hundred and twenty (120) publicly traded companies' 10K annual securities filings across five years time was conducted to assess the extent of information security disclosure and, consequently, to derive the security paradigm adopted by these entities. Less than half of the sample engaged in any information security disclosures in their most recent 10K filings. Of those entities in the sample who disclosed,[11] the entities tended to (1) have disclosed information security risks in their filings five years ago, (2) be technology companies, and (3) have been prosecuted for data breaches.

Part II concludes that the entities in the sample, like current legislation, are

11. These "most recent" 10K filings in the sample are as of August 2004. 10Ks are the most important annual shareholder communication and are intended to present shareholders with a thumbnail sketch of the activities of the entity, during the year, through the eyes of management.

also adopting the inferior paradigm of "security through obscurity" and that information security learning is not emerging as quickly as needed in publicly traded entities. Because of the severity of the information security crisis, entities appear to need legal scaffolding[12] to expedite their transition toward the "security through process" model. This shift will facilitate information security learning, assisting entities in both improving long-term value creation for shareholders and lessening their contribution to the information security crisis.

Part III of this article proposes one type of legal scaffolding that may facilitate the emergence of corporate information security learning. Specifically, Part III proposes a feedback mechanism, theoretically grounded in the cybernetics theory[13] concepts of communication, control, and system, which uses securities regulation to generate an autocatalytic set[14] of self-sustaining good corporate information security behaviors that will ultimately result in better shareholder oversight of corporate activity. The results of this oversight will include systemic improvements in corporate information security and better assurance that corporate information vulnerability, security losses, and diminution of intangible asset value are being correctly factored into the stock price of vulnerable entities. Additionally, a positive externality of such improved corporate security may be that some of these new information security lessons and behaviors will be transferred by employees into their personal behaviors, improving the consumer end of the information security crisis.

I. THE INFORMATION SECURITY CRISIS

During the last decade, our society has undergone an information control revolution driven by technology-mediated networks. In accordance, the business environment within our society has been dramatically altered by the integration of information technology into corporate governance and operations.[15] Furthermore, business communications have progressively shifted

12. Scaffolding is an education theory term which involves facilitating an individual's learning by giving them as little assistance as possible while at the same time ensuring their success. Therefore, the key is to let the learner teach herself while monitoring her progress and providing only as much redirection and correction as needed to keep the learner's progress on target. *See* Irina Verenikina, *Understanding Scaffolding and the ZPD in Education Theory* (2003), http://www.aare.edu.au/03pap/ver03682.pdf. In effect, traditional Socratic teaching methodology, if used correctly, is an example of scaffolding in action—a professor assists the student in teaching herself.

13. For a definition of and discussion of cybernetics, see American Society for Cybernetics, http://www2.gwu.edu/~asc/cyber_definition.html (last visited Jan. 17, 2005); NORBERT WIENER, CYBERNETICS OR CONTROL AND COMMUNICATION IN THE ANIMAL AND THE MACHINE (1948); A.Y. AULIN, CYBERNETIC LAWS OF SOCIAL PROGRESS (1982).

14. An autocatalytic set is a group of elements that work together to generate a product that itself becomes the stimulus for the reaction which generates the next generation product. For a discussion of autocatalysis, see STUART KAUFFMAN, AT HOME IN THE UNIVERSE (1995).

15. For example, most law firms use document management systems to centralize work product. For a discussion of document management software, see Dennis Kennedy & John Gelagin, *Want to Save*

from real space to virtual space[16] and entirely new technology-contingent businesses have arisen, such as eBay and Google.[17] As the digital divide[18] in the United States closes,[19] businesses and consumers have adopted new technologies in their purchasing behaviors[20] and now view the purchasing of goods through the Web as a routine part of life.[21] Unfortunately, as a result of this successful incorporation of network-mediated information technology into corporate and consumer economic behaviors, our society now faces an information security crisis.[22]

A. The Problem

As information technology has weaved into corporate practices and consumer economic behaviors, a new economic environment has emerged with the prevalence of corporate and consumer data collection, aggregation, and leveraging. Corporate proprietary information and personally identifiable

---

16 Minutes Every Day?, FINDLAW, Feb. 2003, http://practice.findlaw.com/archives/worldbeat_0203.html. This use of information technology serves to facilitate knowledge management, the sharing of institutional intellectual resources such as form contracts, and control over access to certain information.

16. Ed Frauenheim, *Report: E-mail Volume Grows Rapidly*, CNET, Oct. 2, 2003, http://news.com.com/2110-1032-5085956.html?tag=3Dnefd_hed.

17. *See* Sharon K. Sandeen, *The Sense and Nonsense of Website Terms of Use Agreements*, 26 HAMLINE L. REV. 499, 508 (2003). As a consequence of this transformation, numerous state corporate statutes have been amended to allow for email notice, virtual shareholder meetings, and internet proxy voting. *See, e.g.*, Gary W. Derrick & Irving L. Faught, *New Developments in Oklahoma Business Entity Law*, 56 OKLA. L. REV. 259, 263-65 (2003); *see also* Robert C. Pozen, *Institutional Perspective on Shareholder Nominations of Corporation Directors*, 59 BUS. LAW. 95 (2003).

18. The term "digital divide" has been used by academics and policymakers to describe the gap that exists within and across countries between information technology "haves" and "have-nots," i.e. those individuals and groups with access to information technology, specifically the Internet, and those individuals without such access. For a discussion of the digital divide, its contours and its relationship to corporate information technology production, see Andrea M. Matwyshyn, *Silicon Ceilings: Information Technology Equity, the Digital Divide and the Gender Gap Among Information Technology Professionals*, 2 NW. J. TECH. & INTELL. PROP. 1 (2003), http://www.law.northwestern.edu/journals/njtip/v2/n1/2.

19. Progress toward universal access is being achieved. Between 1994 and 1998, the number of Americans owning computers increased by over fifty percent, and the number of households using e-mail quadrupled. Between December 1998 and July 2000, the percentage of households with Internet access increased by fifty-eight percent. Over half of all households had computers by July 2000, and individuals using the Internet rose by a third. *See* U.S. Dept. of Commerce, Nat'l Telecomm. & Info. Admin., *Falling Through the Net II: New Data on the Digital Divide* (July 1998), *available at* http://www.ntia.doc.gov/ntiahome/net2/falling.html.

20. For a discussion of consumer technology adoption, see Richard Trinkner & Brian Smith, *Consumer Technology Adoption Roadmap*, Gartner, http://www.gartnerg2.com/site/FileDownload.asp?file=wp-0902-0002.pdf.

21. *See* Press Release, National Statistics (UK), More Businesses Are Buying over the Internet, (Nov. 3, 2004), *available at* http://www.statistics.gov.uk/pdfdir/e-com1104.pdf.

22. For a discussion of the consequences of technological adoption and the values embodied therein, see, for example, EVERETT ROGERS, DIFFUSION OF INNOVATIONS (1995) (discussing the consequences of innovations, examining the value implications of different innovations, and arguing that technologies need to be critically evaluated from utilitarian and moral perspectives before being adopted).

consumer data collected by entities are now centralized into networked databases known as "hubs" of information within business entities.[23] Society thus faces a new set of harms related to failures in information control and security.[24]

The effects of weak information security detrimentally impact multiple levels of social ecology resulting in three types of harms: confidentiality harms, integrity harms, and availability harms. On the macrosystem/societal level,[25] fraud resulting from these harms generates billions of dollars of economic losses in the aggregate and burdens both the marketplace and the legal system. On the mesosystem/interpersonal[26] level, these harms erode commercial trust and cause difficulty in commercial communications. On the microsystem/individual level,[27] these harms hinder commercial identity development for both corporate entities and consumers.

1. Macrosystem: The Social Costs of Weak Information Security

The U.S. economy has lost billions of dollars to information security harms. In 2003 alone, the social costs of information vulnerability totaled approximately $60 billion in the United States.[28] As an illustration of the magnitude of these costs, in view of the notion that identity theft is widely regarded to be severely underreported[29] the total economic costs of reported incidents of identity theft amount to approximately $50 billion per year according to a study commissioned by the Federal Trade Commission (FTC).[30] On average, each act of identity theft results in a loss of $4,800.[31]

The financial burdens resulting from these harms impact not only individual victims, but also our economy and society as a whole. They damage confidentiality interests and the integrity and availability of certain social

23. *See, e.g.*, ALBERTO LASZLO BARABASI, LINKED (2002).

24. In particular, these harms include malicious or unwanted information collection by third parties.

25. Macrosystem level analysis requires examination at the level of culture as a whole, along with belief systems and ideologies underlying cultural rules and norms. In other words, the analysis focuses on the mechanisms of social governance and the worldview prevalent in civil society. *See* URIE BRONFENBRENNER, THE ECOLOGY OF HUMAN DEVELOPMENT 258 (1979).

26. Mesosystem level analysis focuses attention on interpersonal dynamics and the dynamics between individuals and secondary settings, such as work. *Id.* at 209.

27. On the microsystem level, individuals and their psychological development in a particular context is the primary level of analysis. *Id.* at 109.

28. Information security crimes usurp large amounts of social resources. The costs of information crime ripple through the criminal justice system and other parts of society as well as the economy. Costs of prosecution and incarceration of information criminals must be added to the $60 billion+ total economic losses resulting from these information crimes.

29. Robert Lemos, *Analyst: Crime Pays for Identity Thieves*, CNET, July 21, 2003, http://news.com.com/Analyst+Crime+pays+for+identity+thieves/2100-1009_3-5050295.html?tag=nl.

30. FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT (Sept. 2004), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

31. *Id.*

resources. For instance, some social structures, such as the social security system, are contingent on data confidentiality and security of information. A compromise of individuals' social security numbers can result in fraud, which then requires the expenditure of social resources. In addition to the costs of prosecution, such frauds further necessitate the incurring of transaction costs associated with issuing new social security numbers to victims and eliminating the old numbers from the social security rolls. Similarly, the integrity of social structures, such as law enforcement and the criminal justice system, is negatively impacted by information crime. Identity thieves may sometimes identify themselves using a victim's identity when being charged with a crime.[32] Discovering this misidentification of the criminal and clearing up the consequential damage to the victim's record similarly usurps both social and law enforcement resources.

Finally, the availability of social resources, such as work hours used for economic production, is also jeopardized by information crime. Workers frequently repurpose hours from economic activity in the workplace to resolving their personal issues resulting from information crime. The value of the time spent by individual victims in resolving the adverse effects of identity theft approaches 300,000,000 hours per year.[33] These hours could otherwise be devoted to more economic production, purchasing items on the Web, or other socially beneficial ends.

2. Mesosystem: Weak Security and Burdens on Business Entities

On the mesosystem/interpersonal level, information vulnerability and crime erode commercial trust between business partners. Corporate entities suffer economic harms and reputational damage as a consequence of their own or their business partners' inadequate security practices. For example, it is estimated by the Federal Trade Commission that U.S. corporations have lost approximately $48 billion to identity theft alone between September 2002 and September 2003.[34] Confidentiality, integrity, and availability of corporate assets are all negatively impacted by information vulnerability and crime.

Certain corporate assets, such as databases of customer information and

32. *Id.* Approximately 15% of identity theft victims' personal information is fraudulently used in nonfinancial ways, particularly in connection with the thief being charged with a crime and passing himself off as the victim. Four percent of victims reported that their information was misused in this way. *See* Declan McCullagh, *Study: Millions Hit by ID Fraud*, CNET, Sept. 3, 2003, http://news.com.com/Study+Millions+hit+by+ID+fraud/2100-1029_3-5071060.html?tag=st.rc.targ_mb.

33. IDENTITY THEFT SURVEY REPORT, *supra* note 30, at 6.

34. *See* MailFrontier, Threat Stats, http://www.mailfrontier.com/threats/stats.html (last visited Nov. 3, 2005); Press Release, Federal Trade Commission, FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers (Sept. 3, 2003), *available at* http://www.ftc.gov/opa/2003/09/idtheft.htm.

preferences, are valuable only because of their confidentiality.[35] One data breach could greatly diminish the value of such an intangible asset.[36] For example, the damage that a corporate insider can generate in one episode of information theft has been, in at least one instance, approximated to be between $50 million to $100 million.[37] Similarly, corporate proprietary information protected solely by trade secret law could, in effect, lose all its value in an information crime incident because the information's status as a trade secret is entirely contingent upon its confidentiality.[38]

The integrity of corporate systems is additionally in jeopardy as a consequence of suboptimal security. PricewaterhouseCoopers estimates that corporations sustained more than $1.5 trillion in losses in 2000 due to security breaches, such as computer viruses.[39] Corporate integrity is further affected by a parallel diminution in brand value and corporate goodwill. An entity considered to be vulnerable generally suffers a decrease in the value of its investments in brand identity building because it breaches its promises of data care. A brand can become tainted in the minds of business partners and consumers if it is associated with lax information security.[40] Finally, some

35. For example, Acxiom Corporation derives revenue principally from selling aggregated information. If this information is stolen and becomes available cheaply on the information black market, it is highly unlikely that Acxiom will be able to maintain the value of this intangible asset at previous levels.

36. Benjamin Wright, *IT Security Law*, http://www.taxadmin.org/fta/meet/04tech_pres/wright.pdf. In the tax context, entities frequently argue that they should be allowed to amortize the value of their customer lists. *See* Charles Schwab Corp. v. Comm'r, 123 T.C. 306 (2004).

37. In the biggest incidence of identity theft known to date, a help desk worker at Teledata Communications, Inc., which provides credit reports on consumers to lenders, is estimated to have stolen 30,000 consumers' credit reports which he shared with around 20 compatriots who leveraged the data to cause significant financial damage to the consumers in question. He was paid approximately $30 per credit report, or a total of $900,000. *See* Larry Neumeister, *Guilty Plea in Huge ID Theft Case*, CBS NEWS, Sept. 14, 2004, http://www.cbsnews.com/stories/2004/09/15/tech/main643714.shtml; *see also* Reuters, *Man Pleads Guilty in Massive Identity Theft*, CNET, Sept. 15, 2004, http://news.com.com/Man+pleads+guilty+in+massive+identity+theft/2100-1029_3-5367658.html?tag=st.rc.targ_mb.

38. It can be argued that any data leakage is demonstrative of inadequate measures to keep the information secret, thereby putting it outside the scope of trade secret protection of most states' trade secret statutes. Trade secret statutes vary state by state, but most define a "trade secret" as information that an entity has used due care in protecting from disclosure. If it can be demonstrated that information security practices of an entity were suboptimal during any point in the lifetime of the information, it can frequently be successfully argued that the information in question is no longer a trade secret. *See, e.g.*, John T. Soma, Sharon K. Black & Alexander R. Smith, *Antitrust Pitfalls in Licensing*, 449 PLI-PAT 349 (Practising Law Institute—Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, 1996).

39. At least 81,000 viruses are known to be in existence today, poised to generate even more staggering losses. Larisa Epatko, *Cyber Attacks Target Computer Vulnerabilities*, PBS ONLINE NEWSHOUR, http://www.pbs.org/newshour/science/computer_worms/intro.html (last visited Nov. 26, 2004). For example, the Blaster worm losses alone are approaching $10 million. *See* U.S. Dep't of Justice Operation Cybersweep, *available at* http://www.fbi.gov/cyber/cysweep/cysweep1.htm (last visited Nov. 26, 2004).

40. One of the newest brandbuilding techniques is for each entity to make its own corporate cyborg/avatar to provide a friendly face to internet visitors. *See* Vhost Sitepal, http://www.oddcast.com/sitepal/?promotionId=235&bannerId=128 (last visited Nov. 26, 2004).

integrity losses are related to opportunity costs. Occasionally, certain types of vulnerabilities, such as name-your-own-price vulnerabilities,[41] deprive an entity of revenue which it would have otherwise received.

For example, phishing[42] presents a particularly serious threat to corporate entities' goodwill. During a phishing attack, an assailant simultaneously victimizes both entities and their consumers by "spoofing"[43] emails to deceive recipients into believing that the email originated from a credible source with which the consumer may possess a trusted commercial relationship, such as a financial services provider.[44] Phishing attacks frequently include registering domain names that appear to be associated with the targeted entity and otherwise infringing on the intellectual property of the targeted entity. The goal of phishing is to leverage the goodwill[45] of a trusted services provider and trick consumers into revealing personal financial information, usernames, passwords, social security numbers and the like.[46] Phishing fraud losses measured approximately between $500 million to $2.4 billion last year.[47]

Similarly, legitimate email communications from business entities may be ignored by cautious consumers who mistake a legitimate communication for a phishing attack.[48] Consumers victimized by phishing attacks are frequently

---

41. *See, e.g.*, Brian McWilliams, *Name Your Own Price on PayPal*, WIRED NEWS, Apr. 19, 2002, http://www.wired.com/news/business/0,1367,51977,00.html?tw=wn_story_related.

42. The term "phishing" is derived from the idea that Internet con artists use email lures to "fish" for passwords and other personally identifiable data from the sea of Internet users. The letters "ph" are a frequent replacement for "f" in hacker language, and most likely reflect an act of verbal homage to the original form of hacking, called "phreaking," a term coined by the first hacker, John Draper, known as "Cap'n Crunch." By 1996, hacked accounts came to be known as "phish," and by 1997 phish were used as currency by hackers in exchange for items such as hacking software. *See* Anti-Phishing Working Group, http://www.antiphishing.org/word_phish.html (last visited Oct. 9, 2004).

43. Spoofing is defined as sending a message to make it appear as if it is arriving from someone else. *See* Webopedia, http://www.webopedia.com/TERM/I/IP_spoofing.html (last visited Nov. 26, 2004).

44. One entity whose email is spoofed frequently is Citibank. For statistics on phishing see Anti-Phishing Working Group, http://www.antiphishing.org (last visited Nov. 26, 2004). For additional discussion of phishing, see FEDERAL TRADE COMMISSION, PHISHING ALERT, *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm; Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, 12.

45. In particular, phishing attacks usually infringe the trademarks of the spoofed entity as well as the look-and-feel of the entity's website.

46. *Id.*

47. CNET Staff, *Good News: 'Phishing' Scams Net Only $500 Million*, CNET, Sept. 29, 2004, http://news.com.com/Good+news+Phishing+scams+net+ionlyi+500+million/2100-1029_3-5388757.html; *see also* Cynthia L. Webb, *CEOs Plan a Phish Fry*, WASH. POST, June 15, 2004; Press Release, Gartner, Gartner Study Finds Significant Increase in E-Mail Phishing Attacks: Cost to U.S. Banks and Credit Card Issuers Estimated at $1.2 Billion in 2003 (May 6, 2004), *available at* http://www.gartner.com/5_about/press_releases/asset_71087_11.jsp.

48. For example, even a highly technology savvy consumer may have difficulty distinguishing between a phishing email and a legitimate commercial communication from an entity with whom the consumer has a preexisting relationship. *See* MailFrontier Phishing IQ Test II, http://survey.mailfrontier.com/survey/quiztest.html (last visited Nov. 26, 2004). Even the author of this article misidentified one of the items in this quiz, identifying it as fraudulent when, in fact, it was legitimate.

aware that the entity whose email is spoofed is not directly responsible for the phishing attack. Nevertheless, these consumers may form a negative association with the entity, particularly if the victimized entity does not aggressively and publicly pursue the attacker. Thus, phishing presents a severe threat to corporate goodwill as well as to consumer information security.

Lastly, availability of corporate assets also becomes limited as a consequence of security issues. In 2003, corporations spent approximately $11 billion addressing spam-related issues.[49] As an example, spam is usurping companies' server space and worker time.[50] In one study, 34% of email users said they were less able to communicate effectively at work.[51] An attacker may also usurp the quantifiable availability of an entity's technological resources during an attempt to remotely compromise a network. Such resources include, among other things, bandwidth and the work hours allocated to the attack by the people responding to the incident. Incident response employee time does not end when the attack ends as numerous hours are subsequently logged performing forensic examinations, writing incident reports, and fulfilling other recordkeeping obligations. Finally, if a security incident results in a consumer data privacy violation, availability of capital is further diminished because of the subsequent need to cover fines, court costs, attorneys' fees, settlement costs, the bureaucratic costs of setting up compliance mechanisms with consent decrees, settlement agreements, and court decisions.

3. Microsystem: Consumers and Security Related Crime

As more consumers use the internet, the ease of access to a pool of potential victims for information crime increases. As a consequence, consumer information crime will undoubtedly continue to rise, further implicating

49. By comparison, worldwide losses caused by spam in the month of October 2003 alone were approximately $10.4 billion, surpassing viruses and worms, which caused $8.4 billion in losses, and hackers, who caused $1 billion in financial damage. *See* Tim Lemke, *Spam Harmed Economy More than Hackers, Viruses*, WASH. TIMES, Nov. 10, 2003.

50. It is estimated that by the middle of 2004, spam constituted at least 65% of all email. For example, in the experience of at least one entity, the percentage of its inbound email traffic devoted to spam increased to as much as 75% in 2003 from 8% in 2000, and its costs to combat spam increased 700%. *See* DALE W. MALIK, BELLSOUTH INTERNET GROUP, FTC SPAM FORUM NOTES FOR "ECONOMICS OF SPAM" PANEL, http://www.ftc.gov/bcp/workshops/spam/Presentations/malik.pdf. For most users, spam has become such an integral but unwanted part of Internet usage that some spam, like the infamous email allegedly from the son of an ousted Nigerian dictator, has achieved almost a certain cultural status as a communal object of abhorrence, even becoming the subject of a museum exhibit. *See* Heidi Vogy, *Spam Exhibit Turns Inbox Deluge into Art*, INFO. WEEK, Jan. 27, 2004, http://www.informationweek.com; Michelle Delio, *Meet the Nigerian E-Mail Grifters*, WIRED NEWS, July 17, 2002, http://www.wired.com/news/culture/0,1284,53818,00.html; *see also* NIGERIAN LETTER SCAMS, INTERNET FRAUD COMPLAINT CENTER, http://www1.ifccfbi.gov/strategy/nls.asp#Example%20#1 (last visited Jan. 28, 2004); Nigeria 419 Coalition, http://home.rica.net/alphae/419coal/ (last visited Oct. 5, 2004).

51. DEBORAH FALLOWS, PEW INTERNET AND AMERICAN LIFE PROJECT, SPAM: HOW IT IS HURTING EMAIL AND DEGRADING LIFE ON THE INTERNET, http://www.pewinternet.org (last visited Jan. 28, 2004).

confidentiality, integrity, and availability concerns.

Consumers' ability to successfully engage in many commercial activities is contingent upon confidentiality. Consumers usually authenticate their identity through knowledge of "secret" confidential information.[52] Apart from phishing, confidentiality of user information is frequently compromised through what is commonly known as "spyware,"[53] which can be generally defined as any application that sends information to a remote third party. It is estimated that approximately 70%-80% of personal computers today are infected with spyware applications which send confidential user information to unauthorized third parties.[54] Accordingly, when confidential consumer information, such as a credit card number or a social security number, falls into the wrong hands, identity theft is a common result.[55] Not surprisingly, identity theft is considered the fastest-growing crime in the United States.[56] Approximately ten million

---

52. For example, when consumers forget a user name or password to access their bank balances online they engage in an identity authentication process with the bank which ascertains that each consumer is who she says through the consumer's knowledge of confidential or little known information about the consumer, such as the consumer's first pet's name or social security number.

53. Definitions of spyware vary across legislation. For a discussion of spyware legislative efforts, see Reuters, *California Goes After Spyware*, WIRED NEWS, Oct. 2, 2004, http://www.wired.com/news/politics/0,1283,65203,00.html. Spyware can be embedded as part of other products installed by the user. As such, it can bury itself into users' hard drives in a manner which makes them difficult to ferret out and uninstall. Like sniffers, these programs then convey information back to their author. For a discussion of the definitional complexity of spyware, see Wikipedia, http://en.wikipedia.org/wiki/Spyware (last visited Nov. 30, 2004). For a definition of sniffers, see Webopedia, http://www.webopedia.com/TERM/s/sniffer.html (last visited Nov. 30, 2004).

54. *See* Hank Levy, *Measurement and Analysis of Spyware in a University Environment*, http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf; Robert Lemos, *Plague Carriers: Most Users Unaware of PC Infections*, CNET, Oct. 25, 2004, http://news.com.com/Plague+carriers+Most+users+unaware+of+PC+infections/2100-1029_3-5423306.html; *see also* CNET Staff, *Study: Consumers Take Cyberattacks Lightly*, CNET, Sept. 30, 2004, http://news.com.com/Study+Consumers+take+cyberattacks+lightly/2100-7349_3-5390749.html?tag=st.rc.targ_mb.

55. An increasing number of these identity thefts arise out of phishing attacks. During the last year, approximately 57 million people in the U.S., or 20% of the population, have been targeted by a phishing attack. It is estimated that approximately 5% of phishing attempts are successful. *See* Dawn Kawamoto, *U.S. Hit by Rise in Phishing Attacks*, CNET, May 6, 2004, http://news.com.com/U.S.+hit+by+rise+in+phishing+attacks/2100-7355_3-5207297.html?tag=st.rc.targ_mb. Variants of circulating "phishing" e-mails have increased in number from 279 to 215,643 over the past six months. *See* Munir Kotadia, *Phising Scams Lure More Users*, CNET, Apr. 19, 2004, http://news.com.com/%27Phishing%27+scams+luring+more+users/2100-7355_3-5194807.html?tag=st.rn.

56. Simultaneously, however, identity theft is hard to measure accurately because it is severely underreported, with only approximately 25% of victims filing police reports. *See* FEDERAL TRADE COMMISSION, FTC IDENTITY THEFT SURVEY, http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.htm. Meanwhile, state level enforcement in finding perpetrators of identity theft has entailed logistical challenges. According to Chris Hoofnagle of EPIC:

> A big problem in identity theft comes from lack of enforcement. There are problems with state authorities who tend not to want to deal with the problem. If you're a Washington, D.C. resident and someone in California steals your identity, both Washington and California police will play ping-pong with your case to avoid dealing with it. They have other priorities. Enforcement at a federal level may deter the crime and provide the opportunity to capture thieves who are evading state enforcement.

people in the US became victims of identity theft in 2003, which equates to 25% of U.S. households.[57] In 2003-2005, identity theft complaints continued to rise at a rate of over 3% a year.[58]

Incidences of spam,[59] malspam,[60] spyware, and malicious code compromise the integrity and availability of consumers' systems, frequently with "consent" from the user.[61] In particular, the merger of spammers and virus writers[62] now generates a new variant of spam and malspam which intentionally capitalizes on the user's weak information security to siphon data or computing resources from the user without the user's knowledge. With incidences of malspam already at critical levels, the Federal Trade Commission estimates that as much as 30% of all spam currently results from "zombie drones" [63] or security-compromised computers that have been turned into spam platforms controlled remotely by spam senders.[64]

Declan McCullagh, *Season Over for Phishing*, CNET, July 15, 2004, http://news.com.com/Season+over+for+phishing/2100-1028_3-5270077.html?tag=st.rc.targ_mb.

57. Christine Dugan, *Federal Survey: Identity Theft Hits 1 in 4 U.S. Households*, USA TODAY, Sept. 4, 2003.

58. *See* Christopher Conkey, *ID Theft Complaints Still Rising, but Rate Slows*, WALL ST. J., Jan. 26, 2006, at D1.

59. Although the concept of spam is generally contemplated in connection with email, in reality, spam impacts a variety of Internet communications. For example, the first large-scale spam incident occurred on a bulletin board and not through email: a law firm, Canter & Siegel, decided to advertise its immigration law services through a UseNet posting. *See* Peter H. Lewis, *Arizona Lawyers Form Company for Internet Advertising*, N.Y. TIMES, May 7, 1994, *available at* http://www.eff.org/Infra/Commerce_online/lawyers_form_i_company.announce. Spam can also arrive through instant messaging applications and other real time communications. Stefanie Olsen, *Will Instant Messaging Become Instant Spamming?*, CNET, Feb. 16, 2001, http://news.com.com/2100-1023-252765.html?legacy=CNET. Most recently spam has begun to arrive on user desktops as pop-up advertisements even when no browser window is open. *See* John P. Mello, *Feds Obtain Restraining Order Against Super Spammers*, E-COMMERCE TIMES, Nov. 6, 2003, http://www.ecommercetimes.com/perl/story/32069.html.

60. The term MalSpam is this author's coinage. It is intended to refer to malicious spam, meaning spam which capitalizes upon or creates a security vulnerability for either commercial or destructive purposes. *See* Andrea M. Matwyshyn, *Spam and Security: Understanding the Connection Assessing Legal Strategy After the CAN-SPAM Act*, 5 INTERNET L. & BUS. 307, 312 (Mar. 2004).

61. Users unknowingly or carelessly "consent" to the installation of spyware on their machines 80% of the time. *See* Associated Press, *Spyware: Users Say Yes to It*, WIRED NEWS, Oct. 31, 2004, http://www.wired.com/news/privacy/0,1848,65539,00.html?tw=wn_tophead_4. The debate over what constitutes adequate consumer consent is at the crux of the legal debate over the regulation of spyware.

62. Bob Sullivan, *The Secret Tricks Spammers Use*, MSNBC, Aug. 11, 2003, http://www.msnbc.com/id/3078640.

63. Zombie drones are security compromised machines that can be controlled remotely without the user's knowledge and used for sending spam or other malicious purposes. *See Primer: Zombie Drone*, WASH. POST, Feb. 1, 2004. Purchasing spam time on a zombie drone is also relatively inexpensive, costing as little as 3-10 cents per host machine per week. *See For Rent: Hacked Zombie PCs for Net Mischief*, ELECTRIC NEW PAPER, July 13, 2004, http://newpaper.asia1.com.sg/top/story/0,4136,67698-1093276740,00.html; *see also* A New Species: Stefan Savage's Talk at NDSS, http://sunbreaks.blogspot.com (Feb. 4, 2005).

64. David Bank, *New Virus Can Turn You into a Spammer*, WALL ST. J., Jan. 29, 2004. Also a black market has developed for zero-day exploit code to be included or used in connection with spam with the going rate currently set at approximately $4,000-$6,000 per exploit. Zero-day exploit code is code which exploits a security vulnerability for which there is no known patch and of which the vendor

Consumers victimized by information security-related crime suffer both economic integrity harms and the negative psychological feeling of helplessness frequently associated with crime.[65] The pervasiveness of spam has impaired users' sense of control over the availability of their own systems to such an extent that users are starting to use the Internet less frequently.[66] This loss of use arises not only from the annoyance of filtering through their inboxes to find a handful of legitimate messages, but also from fear of fraud: currently, a majority of spam is sent with intent to defraud.[67] Finally, spyware and malicious code can usurp availability and damage integrity of systems in a manner almost invisible to the user. For example, spyware-related problems account for approximately 15% of at least one computer manufacturer's customer availability complaints, up from only 2% in 2003.[68]

Corollary losses by consumers associated with availability and integrity can

---

is not aware. *See* George V. Hulme, *Zero-Day Attacks Expected to Increase*, INFO. WEEK, Mar. 24, 2003, http://www.informationweek.com/story/IWK20030321S0029; Simple Nomad, Comments at the Stanford University Cybersecurity, Research and Disclosure Conference (Nov. 22, 2003). Professional spam senders are also known to be, among other things, authoring increasingly personal looking emails which contain viruses for the explicit purpose of harvesting email addresses to compile saleable databases for the purpose of sending spam. Reuters, *The Beagle Has Landed*, WIRED NEWS, Jan. 20, 2004, www.wired.com/news/infostructure/0,1377,61976,00.html; *see also* Ron Hale, Intrusion Crackdown, http://www.itsecurity.com/papers/telenisus.htm.

65. For example, victims frequently feel residual psychological trauma for as long as five years after a crime. *See* G.M. Herek, J.R. Gillis & J.C. Cogan, *Psychological Sequelae of Hate-Crime Victimization Among Lesbian, Gay, and Bisexual Adults*, 67 J. CONSULTING & CLINICAL PSYCHOL. 945 (1999).

66. FALLOWS, *supra* note 51. To date, the FTC has prosecuted fewer than 100 individuals and entities for spam fraud. *See* Federal Trade Commission, Effectiveness and Enforcement of the CAN-SPAM Act, A Report to Congress, Appendix 5 (2005), *available at* http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf. Most of these enforcement actions involved false content and were brought under Section 5 of the Fair Trade Act, alleging that the defendants in question engaged in unfair trade practices. *See, e.g.*, FTC v. G.M. Funding, No. SACV 02-1026 DOC (C.D. Cal. Nov. 2002); FTC v. Westby, No. 032-3030 (N.D. Ill. Apr. 15, 2003); FTC v. NetSource One, No. 022-3077 (W.D. Ky. Nov. 2, 2002); FTC v. Cyber Data, No. CV 02-2120 LKK (E.D. Cal. Oct. 2002); FTC v. Internet Specialists, No. 302 CV 01722 RNC (D. Conn. Oct. 2002); FTC v. Cella, No. CV-03-3202 (C.D. Cal. May 7, 2003); FTC v. K4 Global Publ'g, Inc., No. 5:03-CV0140-3 (M.D. Ga. May 7, 2003); FTC v. Clickformail.com, Inc., No. 03-C-3033 (N.D. Ill. May 7, 2003).

67. According to the most recent estimates of the Federal Trade Commission, at least 65% of spam contains fraudulent content or attempts to induce the recipient to enter into a fraudulent transaction. In addition to fraudulent content, requests to be removed from spam recipient lists were not honored at least 63% of the time. FEDERAL TRADE COMMISSION, FALSE CLAIMS IN SPAM (2003), http://www.ftc.gov. Spam fraud losses frequently reach as high as $4,000 per victim. The highest median dollar losses reported to the FTC were found among victims of the Nigerian Letter fraud, where losses were approximately $3,864 each. *See* IFCC 2002 INTERNET FRAUD REPORT, http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf.

68. Associated Press, *Spyware: Users Say Yes to It*, *supra* note 61. Malicious code can capitalize on existing security vulnerabilities in software purchased by the consumer "off the shelf." Depending on the nature of the vulnerability, if a malicious actor discovers the vulnerability before it is patched by the consumer, remote compromise is a real danger. Code Red, Code Red II, Nimba, Slammer, Blaster, and Sasser all used remotely exploitable vulnerabilities to take over user machines. Approximately 80% of vulnerabilities discovered in 2004 presented the potential for remote exploitation. NEILS JOHNSON, SYMANTEC, ADMINISTRATION AND SECURITY SOLUTIONS, http://www.lsz-consulting.at/pdf/usa_oktober_04/Symantec_Protect_and_Manage_Sales.pdf.

occur offline as well. For example, individuals take it for granted that they may participate in the social institution of real property ownership provided that they maintain a good credit report. However, an identity theft victim frequently realizes the extent of his/her victimization only at the point when they attempt to obtain a mortgage. At this juncture, a credit report is run and the victim learns that a fraudster has stolen the individual's identity and has already taken out a mortgage in the victim's name.[69] Until the effects of the crime are effectively remedied, property ownership is foreclosed to the victim, and transaction costs accrue to all parties involved in the failed transaction.

B. Recalibrating Information Control After the Technology Revolution

The primary reason our society now faces a pivotal decision point in information control policy is the unprecedented impact of the information technology revolution of the 1990's. Although computing began to take root in non-technology industries during the 1980's and primitive email systems were not uncommon, consumers did not begin to use information technology for communication and commercial purposes en masse until the Internet boom of 1998-2001.[70] The entry of consumers into the Internet space permanently reconfigured the relationship among business entities, consumers, and information criminals. Personally identifiable consumer information became a key corporate asset for many businesses and altered the nature of corporate-consumer information exchange. Simultaneously, entities increasingly realized the efficiency and convenience of corporate data centralization into information networks. Likewise, malicious actors realized the efficiency of targeting these networks for attack by stealing both corporate and consumer information.

These three groups of actors—consumers, corporate entities, and information criminals—currently demonstrate different phases of technology learning and integration. As a consequence, they exist in an unequal power relationship with respect to each other reflective of their disparate levels of technology learning and integration. In order to stem the tide of information theft and improve the stability of the information marketplace, knowledge equalization through technology learning may be required.

1. Disparate Levels of Technology Learning of Consumers, Business Entities, and Information Criminals

According to education theory, the stages of technology learning can be divided into five distinct developmental phases: entry, adoption, adaptation,

69. *See* Press Release, Utah Attorney General, ID Theft + Mortgage Fraud = Utah's Newest Scam (May 19, 2004), http://attorneygeneral.utah.gov/PrRel/prmay192004.htm.

70. For a discussion of consumer email use, see PEW INTERNET AND AMERICAN LIFE PROJECT, REPORT: ONLINE ACTIVITIES AND PURSUITS, http://www.pewinternet.org/report_display.asp?r=106.

appropriation, and invention.[71] The entry phase refers to the stage where the individual is initially introduced to the technology and the resulting transformed physical environment.[72] Incorporation of new technology can be a change agent, stimulating reflection, redesign, and rejuvenation of effective practices.[73] The adoption phase describes the process where the individual begins to accept the technology and tries to integrate it into his or her environment.[74] During the adaptation phase, new technology supports traditional processes and the user begins to see the benefits of this new technology. This visible progress provides a source of satisfaction for users, which then encourages greater incorporation of the technology.[75] In the next stage, the appropriation phase demonstrates a movement toward mastery of the technology, which results in individualization and increasingly more adventurous uses.[76] Finally, the invention phase refers to a state of technology development and integration where the user exhibits a mindset of experimentation, change, and innovation. The user begins to view the technology as a tool[77] in a social interaction where technology knowledge is constructed rather than imparted or transferred.[78] To borrow a key concept of systems theory,[79] the first four phases might be termed "first order" change,[80] and the last might be termed "second order" change.[81] Our society currently

---

71. DAVID C. DWYER, CATHY RINGSTAFF & JUDITH HAYMORE SANDHOLTZ, APPLE CLASSROOMS OF TOMORROW, TEACHER BELIEFS AND PRACTICES, PART I: PATTERNS OF CHANGE THE EVOLUTION OF TEACHERS' INSTRUCTIONAL BELIEFS AND PRACTICES IN HIGH-ACCESS-TO-TECHNOLOGY CLASSROOMS FIRST–FOURTH YEAR FINDINGS, http://images.apple.com/education/k12/leadership/acot/pdf/rpt08.pdf. Another useful framework for adult learning of technology was offered by Russell. Russell asserted that adults pass through six stages on their way to becoming confident when learning new technology, beginning at any point and progressing at their own rates. The stages were (a) awareness but nonuse, (b) learning the process, (c) understanding and application of the process, (d) familiarity and confidence, (e) adaptation to other contexts and viewing a computer as a tool, and (f) creative applications to new contexts. A. L. Russell, *Stages in Learning New Technology*, 25 COMPUTERS IN EDUC. 4, 173-78 (1995).

72. *See* DWYER ET AL., *supra* note 71.

73. In the context of managing environmental issues, the term "adaptive management" has arisen to reflect this dynamic management process. For a discussion of adaptive management theory, see British Columbia Ministry of Forests, http://www.for.gov.bc.ca/hfp/amhome/Amdefs.htm.

74. *See* DWYER ET AL., *supra* note 71.

75. *Id.*

76. *Id.*

77. The term tool is used here in the Contextualist sense of the word. In other words, a "tool" in Contextualist developmental psychology theory refers to any instrument that scaffolds learning and permits an individual to accomplish more than s/he otherwise could. It was coined by developmental psychologist Lev Vygotsky. For a discussion of cultural tools, see LEV VYGOTSKY, THOUGHT AND LANGUAGE (1962).

78. *See* DWYER ET AL., *supra* note 71.

79. For a discussion of systems theory, see Vicki Sauter, Information Systems Analysis: Systems Theory, http://www.umsl.edu/~sauter/analysis/intro/system.htm.

80. Bateson discusses the difference between first order change and second order change. First order change refers to the process of acquiring new skills and learning how to do something new. GREGEORY BATESON, STEPS TO ECOLOGY OF THE MIND 50 (1972).

81. Second order change, for Bateson, refers to learning new methods of learning. As such this kind of change requires a deep structural understanding of a system and its rules. *Id.*

faces an information crisis caused by the mismatch of technology development and integration levels among consumers, business entities, and information criminals.

a. Consumers: Adoption and Adaptation

Consumers are progressing through the steps of first order change, on average hovering around the adoption or adaptation stage, with a minority entering the appropriation stage. They are beginning to successfully incorporate technology into their daily routines in the aggregate, to the point where some consumers actually have trouble disconnecting from their technology tools.[82] Approximately 63% of U.S. consumers now have an Internet connection,[83] and more than half of all U.S. households had computers by July 2000.[84] About 53% of those with an Internet connection, or 68 million people, surf the web on a daily basis. Approximately 45% send email every day, and another 30% use a search engine each day.[85] Over 53 million U.S. adults have published content, responded to posts, posted pictures, shared files, and/or otherwise created Internet content.[86] Therefore, of the approximately 218 million U.S. adults,[87] at least a quarter have already contributed Internet content. This statistic demonstrates that the consumer population is progressing through adoption and adaptation toward the appropriation phase. With time, navigating today's information systems may become second nature to a majority of U.S. consumers, just as with using an automatic teller machine today. However, most consumers have yet to reach this phase.

b. Business Entities: On the Cusp of Appropriation and Invention

Business entities in the aggregate are on the threshold between first and second order change. Business uses of technology are becoming creative and individualized. Information technologies are increasingly integral parts of even the most low-tech manufacturer's operations[88] and customization of corporate software is standard practice. Additionally, new business models have emerged

82. *See Yahoo! and OMD Unveil Findings of Internet Deprivation Study*, WEBPRONEWS, Sept. 27, 2003, http://www.webpronews.com/news/ebusinessnews/wpn-45-20040922YahooandOMDUnveilFindingsofInternetDeprivationStudy.html.

83. *See* Pew Internet and American Life Project, Percent of American Adults Online, http://www.pewinternet.org/trends/InternetAdoption.jpg.

84. *See New Data on the Digital Divide*, *supra* note 19.

85. Pew Internet and American Life Project, Daily Activities, http://www.pewinternet.org/trends/Daily_Activities_4.23.04.htm (last visited Nov. 29, 2004).

86. AMANDA LENHART, DEBORAH FALLOWS & JOHN HORRIGAN, PEW INTERNET AND AMERICAN LIFE PROJECT, CONTENT CREATION ONLINE, http://www.pewinternet.org/pdfs/PIP_Content_Creation_Report.pdf.

87. Press Release, U.S. Census Bureau, Census Bureau Estimates Number of Adults, Older People and School-Age Children in States (Mar. 10, 2004), *available at* http://www.census.gov/Press-Release/www/releases/archives/population/001703.html.

88. *See* Alliance Manufacturing, http://www.alliancemfg.com (last visited Nov. 29, 2004).

that would not have been viable prior to the information technology revolution of the 1990s. For example, numerous business entities now exist with a business model entirely or substantially predicated on the leveraging of consumer data collected through information technology.[89]

This integration of technology into the heart of business management has provoked a fundamental change or paradigm shift[90] in corporate identity. As a consequence, the traditional legal "nexus of contracts"[91] approach and the legal approach of viewing the corporation as the equivalent of a natural person[92] do not adequately conceptualize the dynamic and emergent reality of the corporation. A corporation is more accurately conceptualized as a system with intersecting networks.[93] Corporate entities have organizationally evolved from a structural paradigm[94] with information distributed across the enterprise toward a scale-free network paradigm[95] where information and data flows have been concentrated into "hubs" of centralized information and "nodes" of use throughout the entity. Although data is more centralized, an increasing number of individuals have easy access to more corporate data because of corporate network technology. In other words, corporate identity has been restructured around the architectures of entities' information systems.

This reorganization of corporate information around information systems has precipitated not only a transformation in corporate identity, but also the emergence of new business information risks. Similarly, previously existing risks have been exacerbated. For example, the transaction costs of an act of corporate data theft have decreased due to data centralization. One hack into a

---

89. *See* B. JOSEPH PINE & STAND DAVIS, MASS CUSTOMIZATION: THE NEW FRONTIER IN BUSINESS COMPETITION (1999).

90. *See* THOMAS KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (1962).

91. *See* Reuven S. Avi-Yonah, *Corporation, Society and the State: A Defense of the Corporate Tax*, 90 VA. L. REV. 1193 (2004); Barry D. Baysinger & Henry N. Butler, *Anti-Takeover Amendments, Managerial Entrenchment, and the Contractual Theory of the Corporation*, 71 VA. L. REV. 1257 (1985); Lucian Arye Bebchuk, *The Debate on Contractual Freedom in Corporate Law*, 89 COLUM. L. REV. 1395 (1989); Henry N. Butler, *The Contractual Theory of the Corporation*, 11 GEO. MASON L. REV. 99 (1989); Frank H. Easterbrook & Daniel R. Fischel, *The Corporate Contract*, 89 COLUM. L. REV. 1426 (1989). For a critique of this theory see William W. Bratton, Jr., *The "Nexus of Contracts" Corporation: A Critical Appraisal*, 74 CORNELL L. REV. 407 (1989).

92. *See supra* note 91. But, for a discussion of the historical context of corporate law generally and limited liability, in particular, as an important factor in addition to the standard conceptualization of corporate identity, see Stephen B. Presser, *Thwarting the Killing of the Corporation: Limited Liability, Democracy, and Economics*, 87 NW. U. L. REV. 148 (1992).

93. Corporations are more accurately conceptualized as networks of individuals with bounded rationality which are aggregated into dynamic, nonlinear systems, whose behavior is constrained by, among other things, bundles of contracts. While human agency can shape social systems such as these to generate short term predictability, long term predictability is not possible. *See* David Levy, *Applications and Limitations of Complexity Theory in Organizational Theory and Strategy*, *in* HANDBOOK OF STRATEGIC MANAGEMENT (Jack Rabin, Gerald Miller & W. Bartley Hildreth eds., 2000); David Levy, *Chaos Theory and Strategy: Theory, Application, Management Implications*, 15 STRATEGIC MGMT. J. 167 (1994).

94. BARABASI, *supra* note 23.

95. *Id.*

network can provide hundreds of data files that can be instantly copied and is more difficult to detect as "missing" because of the perfectly duplicable nature of digitally stored information. In the past, stealing the same amount of information required a larger time commitment during the act of theft. Manually photocopying files to avoid detection or physically carrying files out of building was not an expeditious process and required presence onsite. The ease of data transference facilitates greater exchange and leveraging of information with other entities. However, with greater ease of data sharing also comes greater risk of internal data leakage from partners and external attacks from information criminals.

Therefore, when analyzing the level of technology learning and integration of business entities, it can be said that entities are on the cusp of first and second order change. They have successfully incorporated information systems into their operations for the most part and many entities modify their systems to perform customized tasks. As such, entities tend to demonstrate a basic mastery of technology above that of the average consumer and are expeditiously moving toward harnessing technology to innovate.

c. Information Criminals: Information Security Inventors

Information criminals frequently sit squarely in the phase of second order change. They are frequently of superior technological proficiency and, in some cases, represent the bleeding edge of technology research and development. While they innovate in a socially detrimental manner, in many cases they are unquestionably intellectual entrepreneurs.[96] For example, in the context of spam, spammers have adjusted their behavior over time in response to anti-spam efforts, resulting in an information security arms race of sorts between spammers and the anti-spam industry. Information thievery has become highly lucrative for spammers. In fact, some professional spammer employees earn salaries in excess of $100,000 per year while professional spammer entity owners earn millions of dollars per year.[97] Consequently, strong financial incentives exist for spammers to innovate in order to stay in business.

Spammers work to write spam dissemination programs which can circumvent current technological anti-spam protections in place.[98] Simultaneously, the leading minds in the industry, at entities such as Microsoft

96. Phishing attacks are becoming increasingly sophisticated. *See* Vikram Desai, *Phishing—Who's Taking the Bait Now?*, CNET, Nov. 23, 2004, http://news.com.com/Phishing+who's+taking+the+bait+now/2010-7349-5463346.html.

97. Simple Nomad, *supra* note 64.

98. For example, spam messages increasingly include "chaff"—strings of characters that appear randomly generated for the purpose of confusing spam filters, which presume that only a legitimate message would contain such a string. For a discussion of chaff, see Geoff Hulten, Anthony Penta, Gopalakrishnan Seshadrinathan & Manav Mishra, *Trends in Spam Products and Methods* (2004), http://www.ceas.cc/papers-2004/165.pdf.

and Yahoo!, race against them to foil these new spamming products. For instance, when the industry resorted to puzzles that required human input to enable transaction processing, spammers outsourced the human labor of performing these puzzles, called human interactive proofs or HIPs[99] to workers in developing countries.[100] It is part of this evolutionary research and development process of spammers that has also lead to the merger of virus writers with spammers with the ascendancy of malspam and phishing. Information criminals' ability to continue their activities is dependent on their ability to constantly innovate, which they will undoubtedly continue to do successfully.

2. Fixing the Information Security Crisis

As discussed in the previous part, the technology knowledge disparity between consumers, entities, and information criminals creates a complex social policy problem ripe for resolution. A two-pronged solution results. The first prong is to facilitate the learning of entities and consumers regarding good information security practices by raising awareness of the importance of information security. The second prong is to build trust in the new marketplace by driving corporate investment, innovation, and self-monitoring in information security while guaranteeing minimum levels of care as a safety net for consumers.

a. Scaffolding Information Security Knowledge Acquisition: Technical Learning Improvement

Corporate entities and consumers do not yet appear to understand the importance and beneficial consequences of strong information security practices. Both entities and consumers underestimate the severity of the information security risks they face. This prevailing lack of basic information security knowledge manifests itself through certain common information security errors: entities and consumers frequently make rudimentary information security mistakes relating to updating and patching software, physical information access control, social engineering[101] attempts, technical configurations of systems, and password practices. These mistakes leave them vulnerable to attack by malicious third parties and insiders.

---

99. HIPs are security puzzles used to verify that the sender of an email is a human and that the email is not an automatically generated bulk spam email from a machine. *See* Carnegie Mellon, HIPs, http://www.aladdin.cs.cmu.edu/hips (last visited Jan. 28, 2004).

100. *See* SpamCop List, Aug. 16, 2001, http://news.spamcop.net/pipermail/spamcop-list/2001-August/018361.html.

101. Social engineering involves tricking people offline into revealing information to compromise security. *See* Hyperdictionary, http://www.hyperdictionary.com/computing/social+engineering (last visited Nov. 29, 2004).

i. Business Entities

The current state of corporate information security is bleak. A 2004 worldwide information security study of 8,100 information technology professionals conducted by CIO Magazine and PricewaterhouseCoopers (the "PwC Study") revealed that entities' security resources did not grow from 2003 to 2004 and at least 55% of companies surveyed had not measured the effectiveness of their security policies and procedures.[102] Of particular concern is the extent of the secrecy regarding companies' security failures – more than half of the entities included in the survey do not report their security breaches because they believe the information will damage corporate reputation and the share price.[103] Even internal reporting is weak and information security knowledge has not been disbursed throughout the entities, in particular, rarely making its way to the legal department.[104] Therefore, based on this admission of a tendency toward secrecy, it is logical to assume that corporate information security practices are even less stringent than as reported by the professionals in this study. Perhaps most disappointingly, the study indicates that government regulations and potential liability were the leading factors driving security investments and improvements. [105]

The most frequent sources of corporate information vulnerability, as reported by information technology professionals, were hackers (66%) and renegade current and former employees (49%). Hackers frequently gain access to corporate proprietary information because an entity's updating and patching behavior is inconsistent. Despite knowledge of vulnerabilities and access to appropriate patches, corporate entities are not always prompt with patching serious security holes.[106] For example, in one study of system administrator behavior, it was found that systems administrators were not adequately responsive to vulnerability announcements. During a seven week period between the public announcement of a serious vulnerability[107] and the release of a worm that exploited that vulnerability[108] causing significant corporate losses, only 40% of servers with the vulnerability were patched.[109] One of the

102. Lorraine Cosgrove Ware, *CIO Research Reports, The State of Information Security 2004*, CIO, Sept. 1, 2004, http://www2.cio.com/research/surveyreport.cfm?id=75.

103. *Id.*

104. *Id.*

105. *Id.*

106. Robert Lemos, *Study: System Admins Slow to Zap Bugs*, CNET, Nov. 19, 2002, http://news.com.com/Study:+System+admins+slow+to+zap+bugs/2100-1001_3-966398.html. *But see* Reuters, *Experts: Microsoft Security Gets an 'F'*, CNN, Feb. 1, 2003, http://www.cnn.com/2003/TECH/biztech/02/01/microsoft.security.reut (discussing problems with patches and why immediate patching is not necessarily always the correct risk management decision).

107. *Id.*

108. Robert Lemos, *Slapper Worm Smarting Lies*, ZDNET, Sept. 20, 2002, http://news.zdnet.com/2100-1009_22-958758.html.

109. *Id.*

factors identified by the study as a major influence in this unacceptably low patching rate was a lack of adequate corporate resources devoted to information security.[110]

Physical information control is intrinsically interwoven with technological information control. For instance, one common practice used by attackers looking to steal proprietary information is known as "dumpster diving." [111] It is common for corporate espionage to include rummaging through the garbage of competitors[112] in search of carelessly disposed of sensitive information. A variation on the theme of physical information control is protecting against attempts at social engineering, which involve physical space acts of deception to acquire information for use in other attacks.[113] Also, certain network settings and poor password controls can facilitate attempts to compromise networks.[114]

Entities frequently forget that many attackers are internal. As a result, failing to require that employees change passwords on a regular and frequent basis or failing to immediately deactivate employee passwords upon an employee's departure can facilitate a data breach.[115] Furthermore, employees commonly receive inadequate security training[116] and those with access to unnecessarily large amounts of confidential information pose a serious risk.[117]

ii. Consumers

On the whole, consumers are even less knowledgeable and thoughtful about

---

110. *Id.*

111. For example, in one case where an attacker was attempting to gain information about Microsoft Corporation, a woman attempted to purchase the garbage of a pro-Microsoft trade group, offering as much as $500 to each of the two cleaners and $200 for their supervisor. *See* Stuart McClure & Joel Scambray, *Forget the Firewall; Guard Your Garbage Against Dumpster Diving Hackers*, INFOWORLD, http://www.infoworld.com/articles/op/xml/00/07/03/000703opswatch.html.

112. In this type of attack, the preferred targets for rummaging through trash are dumpsters, as the term suggests, or wastebaskets accessed through bribed cleaning staff. On occasion, however, breaking and entering has been used as well to secure information. *Id.*

113. For example, a group of hackers called the Phonemasters is known to have penetrated systems at AT&T, MCI WorldCom, Sprint, Equifax, TRW, and the databases of Lexis-Nexis and Dun & Bradstreet using techniques involving mostly dumpster diving and social engineering. *Id.*

114. For example, networks frequently emit information about their specifications and users to any third parties who query for such information for the alleged purpose of client authentication. For a discussion of client authentication protocols, see, for example, Kevin Fu, Emil Sit, Kendra Smith & Nick Feamster, *Do's and Dont's of Client Authentication on the Web*, http://www.pdos.lcs.mit.edu/papers/webauth:sec10.pdf; Cem Paya, *A Framework for Network Authentication Protocols*, http://www.cs.dartmouth.edu/reports/abstracts/TR98-328/.

115. Employees were second only to hackers as sources of information vulnerability according to the PwC Study. *See* Ware, *supra* note 102.

116. *See* ERNST & YOUNG, 2004 GLOBAL INFORMATION SECURITY SURVEY, http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf.

117. The corporate practice of granting "least privilege" could alleviate a portion of this problem. For example, a help desk worker at AOL sold the entirety of AOL's subscriber database to a spammer. *See* Bob Sullivan, *AOL Customer List Stolen, Sold to Spammer*, MSNBC, June 24, 2004, http://www.msnbc.msn.com/id/5279826/.

information security than business entities. Consumers with lax information security behaviors, who use always-on connections[118] with high bandwidth,[119] become particularly attractive targets to malicious third parties for remote compromise. For example, according to research from Dartmouth compiling several studies on undergraduates,[120] although over 50% of users stated that they were worried about information security, 58% rarely or never looked for browser security signals before submitting their confidential information through the Web.[121] 60% of users updated their anti-virus software less frequently than once a month. [122] Over 50% have shared their passwords, 65% never changed their passwords, and another 36% used the same password for all their applications and websites.[123] Poor password management makes consumers especially vulnerable to identity theft.[124]

Similarly, in a recent survey of consumers regarding their information practices, more than 30% believed they had a higher likelihood of winning the lottery than being victimized by malicious code, and only 60% knew the last time they updated their security software.[125] In reality, of course, the risks highlighted in the part above are severe: industry projections estimate that consumer Internet users will be exposed to approximately 100,000 various pieces of malicious code in a year's time. [126] By failing to protect themselves, users have defaulted, perhaps unwisely, to trusting the system and the reputation of the corporate entities with whom they do business. This statistical data demonstrates that consumers expect technology to be secure, want assurances that the system will not fail, and generally favor regulation.[127]

---

118. Always-on connections are high bandwidth connections perpetually connected to the Internet. Consumers who have always-on connections but do not patch their systems regularly present particularly attractive targets for being turned into zombie drones. *See* Press Release, Federal Trade Commission, Pop-up Ad Spammers Settle FTC Charges (Aug. 9, 2004), http://www.ftc.gov/opa/2004/08/dsquared.htm; *see also* FTC v. D Squared Solutions, LLC, No. AMD 03 CV 3108, 2003 WL 22881377 (D. Md. Oct. 30, 2003).

119. *Id.*

120. Denise Anthony, *User Security Behavior* (July 2004) (presented at Dartmouth College PKI Unlocked Summit), http://www.dartmouth.edu/~deploypki/summit04/presentations/PKIUserBehavior.ppt#37.

121. *Id.*

122. *Id.*

123. *Id.*

124. Dinesh C. Sharma, *Study: Identity Theft Worries Consumers*, CNET, Feb. 25, 2004, http://news.com.com/Study+Identity+theft+worries+consumers/2100-7355_3-5165044.html?tag=st.rc.targ_mb.

125. By comparison, 90% knew the name of the performer at the last Super Bowl halftime show. CNET Staff, *Study: Consumers Take Cyberattacks Lightly*, CNET, Sept. 30, 2004, http://news.com.com/Study+Consumers+take+cyberattacks+lightly/2100-7349_3-5390749.html?tag=st.rc.targ_mb.

126. *Id.*

127. *Id.*; *see also* Anthony, *supra* note 120.

b. Setting Minimum Legal Standards for Information Security

Within this context, Congress has begun to legislate information security through the Children's Online Privacy Protection Act, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and the Controlling the Assault of Non-Solicited Pornography and Marketing Act.[128] Congress is, in part, legislating to facilitate the development of minimum standards of data care, as will be discussed in the next part. Another part of this burgeoning information security legislative effort, however, is a public relations campaign: Congress hopes to bring attention to the importance of information security and to scaffold the learning of both consumers and entities with regard to good information security practices.

As mentioned previously, government regulations and potential liability are the leading factors driving security investments and improvements by entities according to information security professionals.[129] The source of this concern by corporations arises from the increasing momentum of Congressional and regulatory agency information security initiatives since the turn of the 21st century. For example, in 2002, the Federal Trade Commission designated October 27 as National Cybersecurity Day.[130] By comparison, in 2004, the entire month of October has been designated as National Information Security Month.[131] Legislation to date has spanned four primary types of data—children's data, health data, financial data, and email data.

i. COPPA

Children's data collection was addressed by Congress in 1998 in the Children's Online Privacy Protection Act ("COPPA").[132] COPPA requires that websites targeting children under age thirteen provide notice of their privacy practices and obtain verifiable parental consent prior to collecting data from the

---

128. The Identity Theft Penalty Enhancement Act ("ITPEA") was also signed into law on July 15, 2004. Public Law 108-275, 118 Stat. 831 (2004). The Act amended Chapter 47 of Title 18 to create an offense of "aggravated identity theft" that refers to the knowing transfer, possession, or use of a means of identification of another person without permission. ITPEA provides for a term of imprisonment of 2 years in addition to the terms awarded for the accompanying felony. States have also begun to legislate more vigorously with respect to identity theft. For example, California recently passed the most protective privacy legislation in the country, requiring financial institutions to inform consumers of data breaches. *See* Robert Lemos, *Law Aims to Reduce Identity Theft*, CNET, June 30, 2003, http://news.com.com/Law+aims+to+reduce+identity+theft/2100-1017_3-1022341.html?tag=st.rc.targ_mb; *see also* Declan McCullagh, *Season Over for Phishing*, CNET, July 15, 2004, http://news.com.com/Season+over+for+phishing/2100-1028_3-5270077.html?tag=st.rc.targ_mb.

129. Ware, *supra* note 102.

130. *See* Press Release, Federal Trade Commission, Turn Back the Clock and Move Forward with Internet Security (Oct. 23, 2002), http://www.ftc.gov/opa/2002/10/cybersecurityma.htm.

131. *See* Federal Trade Commission, Consumer Information: National Cyber Security Awareness Month (Oct. 2004), http://www.ftc.gov/bcp/conline/edcams/infosecurity/ncsa.html.

132. 15 U.S.C. §§ 6501-6506 (2004); *see also* Children's Online Privacy Protection Rule, 16 C.F.R. pt. 312 (2004).

child. The statute also empowers the Federal Trade Commission to promulgate additional regulations requiring the operator of a website subject to COPPA to establish and maintain reasonable procedures "to protect the confidentiality, security, and integrity of personal information collected from children."[133] Additional regulations state that the appropriate security measures for protecting children's data include "using secure web servers and firewalls; deleting personal information once it is no longer being used; limiting employee access to data and providing those employees with data-handling training; and carefully screening the third parties to whom such information is disclosed."[134] However, encryption was deemed to be potentially cost prohibitive and left to the discretion of the entities, as was the use of contractual provisions requiring minimum standards of data care from third parties who have been granted access to the collected children's data.[135] In other words, COPPA leaves much discretion in data security to the individual website operator and creates no external reporting mechanism to monitor internal security improvements.

ii. HIPAA

In the area of health data privacy, the Health Insurance Portability and Accountability Act ("HIPAA") was passed and signed into law in 1996 to provide a framework for, among other things, minimum levels of data care and security with regard to the collection, storage, and sharing of personally identifiable health information.[136] Specifically, HIPAA requires that entities "covered"[137] by HIPAA, who are handling personally identifiable health information, provide notice of privacy practices and ensure the privacy and security of the information.[138] HIPPA's administrative simplification rules can be divided into three segments: privacy rules, which took effect in April, 2003; transaction rules, which took effect October, 2003; and security rules, which

133. 15 U.S.C. § 6502(b)(1)(D) (2004).

134. 16 C.F.R. pt. 312.8 (2004), *available at* http://www.ftc.gov/os/1999/10/64fr59888.pdf. Sadly, this articulation of the proper technology specifications is suboptimal. For example, the implementing regulations instruct companies to use "secure servers"; servers cannot be inherently "secure" or "vulnerable." Securing a server is a process that is ongoing. Perhaps a better phraseology would be to have required companies to take all steps identified by a leading security research firm as fundamental to the exercise of care in attempting to secure a server on an ongoing basis.

135. *Id.*

136. Health Insurance Portability & Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996); *see* U.S. DEPARTMENT OF LABOR, FACT SHEET: HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT, http://www.dol.gov/ebsa/newsroom/fshipaa.html (last visited Nov. 30, 2004). For a discussion of HIPAA, see Mary Beth Johnston & Leighton Roper, *HIPAA Becomes Reality: Compliance with New Privacy, Security and Electronic Transmission Standards*, 103 W. VA. L. REV. 541 (2001). *See also* Peter P. Swire & Lauren B. Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515 (2002).

137. Covered entities include health care providers, health information clearinghouses, and health plans. 45 C.F.R. § 160.103 (2004).

138. 45 C.F.R. § 164.520 (2004).

were published in the Federal Register on February 20, 2003,[139] and become effective for enforcement purposes on April 21, 2005.[140] Additionally, the final security rules mandate that covered entities implement administrative, physical, and technical safeguards.[141] In particular, the HIPAA privacy rules require that responsibility for privacy within each organization be centralized in a Chief Privacy Officer.[142] Also, both the HIPAA privacy[143] and security rules mandate disclosure of practices to consumers and require that contracts with third party providers include a warranty on the part of the provider to maintain the integrity, confidentiality, and availability of health data they receive.[144]

iii. GLBA

Financial information privacy was addressed by the Gramm-Leach-Bliley Act ("GLBA"), also known as the Financial Modernization Act of 1999.[145] GLBA governs the data handling of "financial institutions"[146] broadly defined. It requires that financial institutions provide notice of privacy practices and exercise care in data handling, including granting consumers the opportunity to opt out of data sharing and prohibiting the use of consumer financial information in ways not authorized by the consumer.[147] GLBA also imposes an obligation on financial institutions to enter into contracts with commercial partners with whom they share data, pursuant to an exemption under the act. These contracts must prohibit the partner's' use of customer information for

139. *See* Health Insurance Reform: Security Standards, 45 C.F.R. pts. 160, 162, 164 (2004), *available at* http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf.

140. 45 C.F.R. § 160.308 (2004).

141. *See* 45 C.F.R. pts. 160, 162, 164; PRICE WATERHOUSE COOPERS, HOW HIPAA AND SECURITY INTERSECT: REPORTING ON REQUEST, http://www.pwcglobal.com/extweb/manissue.nsf/DocID/67B8EB4D694ACC0685256DE8007EC9F6 (last visited Nov. 30, 2004).

142. Under § 164.530, entities are required to designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity and a contact person or office who is responsible for receiving complaints. *See* Health Insurance Reform: Security Standards, 45 C.F.R. § 164.530(a) (2004), *available at* http://aspe.hhs.gov/admnsimp/final/PvcTxt01.htm. The role of the Chief Privacy Officer is in flux. Many companies not involved in handling health information have also begun to designate officer level privacy positions. PRICE WATERHOUSE COOPERS, *supra* note 141.

143. 45 C.F.R. §§ 164.502(e), 164.504(e) (2004).

144. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8359 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164 (2004)), *available at* http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf.

145. 15 U.S.C. §§ 6801-6809 (2004).

146. The term "financial institutions" as used by the GLBA refers to entities that offer financial products or services to individuals, such as loans, financial or investment advice, or insurance, including non-bank mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, real estate settlement services providers, and debt collectors. *See* FEDERAL TRADE COMMISSION, IN BRIEF: THE FINANCIAL PRIVACY REQUIREMENTS OF THE GRAMM-LEACH-BLILEY ACT, http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.pdf. (last visited Feb. 6, 2006).

147. *See* Alternative Forms of Privacy Notices Under the Gramm-Leach-Bliley Act, 68 Fed. Reg. 75164 (proposed Dec. 30, 2003) (to be codified at 16 C.F.R. pt. 313), *available at* http://www.ftc.gov/os/2003/12/031223anprfinalglbnotices.pdf.

any purpose other than that of the initial disclosure of information.[148] However, few entities have ever been prosecuted for violations of GLBA and GLBA privacy notices have received sufficient criticism within the privacy community to warrant new proposed rules regarding the format of GLBA disclosure statements.[149]

iv. CANSPAM

In late 2003, Congress passed legislation to create national uniformity in the regulation of spam. The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM),[150] which became effective as of January 1, 2004,[151] prohibits fraudulent or deceptive sender, subject, or content information as well as dictionary attacks[152] and address harvesting.[153] It also requires that the option to opt-out from future mailings be provided in spam email, that such requests be honored, and that sexually explicit materials are clearly labeled as such.[154] Despite the Act's creation of a private right of action for Internet Service Providers ("ISPs"),[155] the Act preempts most state spam statutes in whole or at least in substantial part.[156] As such, it removes

148. 16 C.F.R. § 313.13 (2004), *available at* http://www.ftc.gov/os/2000/05/65fr33645.pdf.

149. *See* Press Release, Federal Trade Commission, FTC Enforces GLBA's Rule Safeguards Against Mortgage Companies (Nov. 16, 2004), http://www.ftc.gov/opa/2004/11/ns.htm.

150. 15 U.S.C.A. § 7701 (West 2003).

151. Four major technological methods have been used to attempt to regulate spam: accept or white lists, deny lists, filtering, and the addition of email "postage" to each message. White lists entail the maintenance of a list of permitted senders and excluding messages not from these permitted senders. *See* John Bone, *AT&T Aborts Plans to Block Email*, MSNBC, Oct. 22, 2003, http://www.msnbc.msn.com/id/3341685. The second method, deny lists, uses rules to refuse acceptance of communication from certain forbidden parties considered to be "bad actors." *See* Jane Waever, *How to End Spam in the Future*, MSNBC, July 9, 2003, http://www.msnbc.msn.com/id/3078599. A third method uses filters based on neural networks or Bayesian networks which are taught to distinguish spam from nonspam. *Id.* The final method involves imposing costs on senders of spam through "postage." Postage comes in various forms—micropayments, "hashcash," which extracts computational costs from senders through solving puzzles that burn CPU cycles, and challenge-response models, which require human attention time. Multiple methods can also be used in tandem. Currently, no reliable system of micropayments exists. *See* Win Treese, *Putting It Together: Where Are the Micropayments*, 7 NETWORKER 3, 15-17 (2003), *available at* http://delivery.acm.org/10.1145/950000/940840/p15-treese.html?key1=940840&key2=4583595701&coll=GUIDE&dl=ACM&CFID=16535447&CFTOKEN=93848377 (last visited Nov. 30, 2004). For a discussion of hashcash, see ADAM BACK, HASHCASH: A DENIAL OF SERVICE COUNTERMEASURE (2002), http://www.hashcash.org/hashcash.pdf. In the context of spam emails, the favored technological method of the moment is imposing a challenge-response model on an unverified sender, such as Human Interactive Proofs. *See* Carnegie Mellon, HIPs, *supra* note 99; Evan Hansen, *Hotmail Tools Fight War Against Spam*, ZDNET, May 8, 2003, http://news.zdnet.co.uk/business/legal/0,39020651,2134436,00.htm.

152. Dictionary attacks are a type of attack where all possible combinations of passwords or randomly generated email addresses are used to attempt to gain access to a protected resource or existing email accounts. *See, e.g.*, Weboepedia, http://www.webopedia.com/TERM/D/dictionary_attack.html (last visited Feb. 6, 2006).

153. 15 U.S.C.A. § 7705 (West 2003).

154. *Id.*

155. 15 U.S.C.A. § 7707(g) (West 2003).

156. While states have also begun to regulate in this space, the CANSPAM Act has superseded any state statutes which regulate the same type of conduct as the Act. As of December 2003, 31 states had

private rights of action granted by some state anti-spam statutes in which ISP's, non-ISP businesses, and consumers previously obtained effective recourse against spammers.[157] Critically, the Act has received mixed reviews at best[158] and leaves many loopholes which may eventually catalyze a boom in certain types of spam.[159]

v. Enforcement

As demonstrated by the legislation described above, Congress has actively attempted to address the information security crisis. However, enforcement actions to support these legislative efforts have not been plentiful. For example, the Federal Trade Commission has prosecuted fewer than 20 entities, to date, for violations of COPPA and their stated privacy policies.[160] As a result of

---

laws regulating the transmission of spam email. None of these statutes contained an outright ban on spam email, but they either (1) restricted either the categories of recipients of spam email to those with a preexisting relationship with the sender or to those who otherwise affirmatively consented to spam email or (2) required clear labeling through a subject line containing the letters ADV, or an opt-out method in the text of the spam to prevent future spam email from being sent to the recipient. With a few exceptions, these statutes were largely unenforced by state attorney generals and few suits were brought under them by recipients until recently. *See* Paul Roberts, *Earthlink Wins $16 Million in Spam Case*, PC WORLD, May 7, 2003, http://www.pcworld.com/news/article/0,aid,110627,00.asp. Cases making use of state level anti-spam email statutes as the basis for suit have been relatively sparse, with no more than a few per state. *See, e.g.*, Microsoft Corp. v. Does 1-50, No. 5:03-cv-00644 (N.D. Cal. Feb. 14, 2003); Hypertouch v. Link It Software Corp., No. CIV426832 (Cal. Super. Ct. Oct. 31, 2002); Morrison & Foerster LLP v. Etracks.com, Inc., No. CIV404294 (Cal. Super. Ct. June 26, 2002); Earthlink Inc. v. Doe, No. 1:01-cv-2097 (N.D. Ga. Aug. 7, 2001); Earthlink, Inc. v. Smith, No.1:01-cv-2009 (N.D. Ga. Aug. 7, 2001); MonsterHut Inc. v. PaeTec Commc'ns, Inc., No. 107189-cv-2001 (N.Y. Sup. Ct. Aug. 27, 2001), *aff'd*, 741 N.Y.S.2d 820 (App. Div. 2002); People v. MonsterHut, Inc., (N.Y. Sup. Ct. Feb. 3, 2003); Verizon Online Servs., Inc. v. Ralsky, No. 01-432-A (E.D. Va. June 7, 2001); Am. Online, Inc. v. CN Prods. Inc., No. 98-552-A (E.D. Va. Nov. 6, 1998); Gilman v. Sprint Commc'ns, No. 020406640 (Utah Dist. Ct. May 22, 2002); State v. Heckel, ,No. 98-2-25480-7 SEA (Wash. Super. Ct. Mar. 10, 2000). In fact, in *Cyber Promotions, Inc. v. America Online, Inc.*, it was the sender of spam who sued AOL alleging that AOL's blocking of spam constituted an infringement of its First Amendment rights. 948 F. Supp. 436 (E.D. Pa. 1995). The court found in favor of AOL, reasoning that AOL was not an instrumentality of the government and did not perform a traditional government function. *Id.* Similarly, the California and Washington anti-spam email statutes were tested on dormant commerce clause grounds and upheld. *See* Ferguson v. Friendfinders, Inc., 115 Cal. Rptr. 2d 258 (Ct. App. 2002); State v. Heckel, 24 P.3d 404 (Wash. 2001).

157. *See* Paul Queary, *Redmond Man Wins Big in Spam Case*, SEATTLE TIMES, Sept. 11, 2003, http://archives.seattletimes.nwsource.com/cgi-bin/texis.cgi/web/vortex/display?slug=spam11&date=20030911.

158. *See* Chris Ulbricht, *Spam Law Generates Confusion*, WIRED NEWS, Jan. 26, 2004, http://www.wired.com/news/business/1,62031-0.html.

159. The most significant loophole in the Act arises as a consequence of its overly narrow definition of the covered forms of spam ; the Act is limited to email only. 15 U.S.C.A. § 7702 (West 2003). As such, it has already failed to be adequately technologically neutral to successfully limit the next generation of spam - malspam. Though a positive step in at least starting a discourse on the issue of spam and ethical marketing practices, the CANSPAM Act will ultimately most likely be of limited effectiveness. Among its other provisions, the CANSPAM Act empowers the FTC to create a Do Not Spam registry. 15 U.S.C.A. § 7709 (West 2003). This centralized information database may become an attractive data harvesting source for spammers if not carefully architected.

160. *See, e.g.*, U.S. v. Hershey Foods Corp., No. 4:03-cv-00350-JEJ (M.D. Pa. Feb. 26, 2003); U.S. v. Mrs. Fields Famous Brands, Inc., No. 2:03cv00205 (D. Utah Feb. 25, 2003); *In re* Eli Lilly & Co., No. C-4047 (F.T.C. May 8, 2002); *In re* Microsoft Corp., No. 012-3240 (F.T.C. Aug. 8, 2002).

these matters, the FTC has levied fines as high as $80,000.[161] With regard to HIPAA, concern exists that enforcement will continue to be weak. At a Department of Health and Human Services (HHS) conference on the HIPAA privacy rule, Office of Civil Rights Director Richard Campanelli stated that HHS will not be aggressive in punishing healthcare organizations that violate HIPAA. Campanelli stated that voluntary compliance is the most effective way to implement data security and recommended that the public complain to the covered entity about privacy breaches.[162]

In contrast, the responses of information security professionals in the PwC Study demonstrate that corporate security improves with an increase in the fear of prosecution. Therefore, active enforcement efforts are an important component of a successful data security regime. Simultaneously, agency resources for enforcement actions are bounded and the problems of information vulnerability are daunting. For example, it is estimated that 15 billion pieces of spam are sent out daily[163] and, to date, the FTC has only prosecuted approximately 60 individuals and entities for spam fraud.[164] If the FTC's estimates are correct and approximately 65% of spam is fraudulent,[165] the scope of the problem is of immense proportions and may be well beyond the control of any government agency.

The current regulatory approach to information security and the present levels of prosecutions for data privacy violations will not adequately address the worsening information security crisis. A new approach is needed to buttress

---

161. *Id.*

162. *See* Phoenix Health Care HIPPAdvisory HIPPAlert, http://www.hipaadvisory.com/alert/vol4/number2.htm (last visited Feb. 6, 2006). Meanwhile, privacy breaches of health records are becoming frequent. For example, an automated probe compromised a computer at Indiana University's Center for Sleep Disorders in November 2003 compromising as many as 7,000 patients' data. *Id.* Similarly, about 1.4 million files containing the personal data of patients may have been stolen from the University of California, Berkeley during a recent security breach. *See* Clea Benson, *Computer Data on Home Care Breached*, SACRAMENTO BEE, Oct. 20, 2004, at A5, *available at* http://www.sacbee.com/content/news/medical/story/11152364p-12068658c.html. Also, incidents have been reported where domestic entities have outsourced work with patient data to entities in other countries and received threats of publishing the patient data on the Web unless the domestic entity paid a "ransom" to prevent disclosure of patient records. *See* PRICE WATERHOUSE COOPERS, *supra* note 141. That said, the first criminal prosecution under HIPAA was settled in August 2004 in an egregious case of patient information theft by an insider who used patient data to obtain credit cards. *See* Press Release, U.S. Dep't of Justice (Aug. 19, 2004), http://www.usdoj.gov/usao/waw/press_room/2004/aug/gibson.htm.

163. *See* Press Release, U.S. Dep't of Justice, *supra* note 162.

164. *Hearings*, *supra* note 57 Most of these enforcement actions involved false content and were brought under Section 5 of the Fair Trade Act alleging that the defendants in question engaged in unfair trade practices. *See, e.g.*, FTC v. Westby, No. 032-3030 (N.D. Ill. filed Apr. 15, 2003); FTC v. NetSource One, No. 022-3077 (W.D. Ky. filed Nov. 2, 2002); FTC v. Scott, No. CV 02-2120 LKK (E.D. Cal. Oct. 3, 2002); FTC v. Lockery, No. 302 CV 01722 RNC (D. Conn. Oct. 4, 2002); FTC v. Cella, No. CV-03-3202 (C.D. Cal. filed May 7, 2003); FTC v. K4 Global Publ'g, Inc., No. 5:03-CV0140-3 (M.D. Ga. filed May 7, 2003); FTC v. Clickformail.com, Inc., No. 03-C-3033 (N.D. Ill. filed May 7, 2003).

165. DIVISION OF MARKETING PRACTICES, FEDERAL TRADE COMMISSION, FALSE CLAIMS IN SPAM (2003), http://www.ftc.gov/reports/spam/030429spamreport.pdf.

existing legal information security structures. The subsequent parts present one such new approach.[166]

II. UNDERSTANDING INFORMATION SECURITY REGULATION IN A COMPLEX SYSTEM

Despite the efforts of Congress and the Federal Trade Commission discussed in the previous part, the severity of the information security crisis is increasing. Part of the reason for this deteriorating state of information security rests in two suboptimal properties of the current regulatory approach: (1) the adoption of an ineffectual paradigm of "security through obscurity," and (2) a lack of leveraging of the dynamic structural properties of networks.

First, the security paradigm adopted by current corporate information security statutes, described in the preceding part, is predicated on a concept known in the technology community as "security through obscurity," which has been generally discredited as an effective security paradigm.[167] This paradigm should be rejected in favor of a paradigm based on process and greater transparency. Second, the current regulatory approach imperfectly conceptualizes the manner in which information systems must be structured for maximizing security and inadequately conceives of the manner in which networks transmit information most effectively—through hubs. Even assuming, however, that government regulation has adopted an inferior paradigm, if the economic hubs of our society have adopted a good security paradigm, this improved security will eventually filter through the system. In such a case, correcting the legislative imperfection may not be necessary. Consequently, an empirical analysis of the security disclosure practices of economic hubs and publicly traded companies assessed the information security paradigm being adopted by these entities in their operations.[168] The entities in the sample had adopted the suboptimal paradigm of "security through obscurity," rather than the superior paradigm of "security through process," thereby demonstrating that information security learning is not adequately emerging in the private sector. Rather, these entities need regulatory assistance to teach them to be more vigilant in their information security practices.

166. For a discussion of the current state of criminal computer intrusion statutes, see Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003). *See also* Neal Kumar Katyal, *Digital Architecture as Crime Control*, 112 YALE L.J. 2261 (2003).

167. *See* Hyperdictionary, http://www.hyperdictionary.com/computing/security+through+obscurity (last visited Nov. 29, 2004).

168. See *infra* Part II.B.

A. Adopting Kerckhoff's Law and a Network-Wide Process-Based Security Regulation Paradigm

The initial critical step to correcting the information security crisis is simultaneously securing the most vulnerable points in the economy while raising the average level of information security throughout the economy as a whole. Though current statutory approaches attempt to address some of the most vulnerable points, they neglect to consider the system as a whole or to provide a means of monitoring progress in security practices. Therefore, it can be argued that Congress has erroneously adopted the information security and cryptography paradigm of "security through obscurity" as the dominant regulatory paradigm in information security legislation. This paradigm should be replaced with a paradigm based on "security through process," considering the dynamics of information transfer in networks.

1. Rejecting Security Through Obscurity as a Regulatory Paradigm

As described in the preceding parts, Congress has been active in legislating improved corporate information security practices. Although the current statutory frameworks provide a good starting point for working to remedy the information security crisis, they will not prove adequate by themselves. The reason existing statutes will prove inadequate stems from their faulty premises: the current legal approach to data security regulation is unconsciously predicated on "security through obscurity," an information security paradigm now widely discredited in the information security and cryptography community.[169]

a. Defining Security Through Obscurity

"Security through obscurity" is the idea that adequate security should be driven by the subjective beliefs of the owners of a system regarding the security of that system. Therefore, if the owners believe that particular security flaws of the system are not widely known or inconsequential, then attackers are unlikely to find and exploit them as long as the owners keep information about the vulnerabilities secret.[170] In other words, the owners' technological knowledge of the system is presumed to be superior to that of hackers under this paradigm. It is also presumed that hackers are not skilled enough to independently acquire the requisite knowledge of such vulnerabilities in the system. Consequently, a "security through obscurity" legislative paradigm reasons that no regular public accountability mechanisms for security are necessary because owners will, for

169. "Security through obscurity" is discredited in the tech community. *See* The Swirl Project: Effective Security Through Visualization, www.isr.uci.edu/projects/swirl/ (last visited Nov. 29, 2004).

170. *See* Brainy Encyclopedia, http://www.brainyencyclopedia.com/encyclopedia/s/se/security_through_obscurity.html (last visited Nov. 29, 2004).

the most part, be vigilant about securing their systems. Therefore, the principle of "security through obscurity" is, in the best case, based on the notion that entities inherently act responsibly with regard to information security and can be trusted to correct any known flaws on their own. However, in the worst case, "security through obscurity" means that if no one discusses security vulnerability publicly, it can be entirely ignored by an entity and not remedied.

The current statutory regime adopts this paradigm. Although information security statutes mandate that corporations take action to protect collected information (particularly consumer information), no provisions create public accountability mechanisms, aside from statutorily empowering the Federal Trade Commission and other agencies to institute regulatory actions. In several cases over the last five years, FTC prosecutions of vulnerable entities were the result of direct or indirect tips from hackers themselves.[171] These prosecutions are frequently the only sources of information available. At best, such a scheme is a highly unsystematic mechanism with questionable ethical implications. Information gathering about potential breaches of security is labor and cost intensive and monitoring companies' security practices on an ongoing basis is a practical impossibility even for a well-funded security-specific agency, something which the FTC is clearly not. Further, in light of severely constrained agency resources, only a small number of regulatory actions will be brought. Therefore, the current regulatory approach essentially relies on the idea that entities will keep their information secure in undisclosed ways and that they will behave responsibly to ensure vulnerabilities are fixed.

b. Why Legislative Adoption of a "Security Through Obscurity" Paradigm is Misguided

A legislative approach premised on the paradigm of "security through obscurity" ignores the realities of the business world. As articulated by information technology professionals themselves, it is fear of liability that catalyzes their companies' improvements in information security. Companies are unlikely to choose to comply to the best of their ability with legislation they perceive to be unclear and onerous, particularly when they are not required to provide any evidence of compliance.[172] If companies are allowed to keep all security-related information secret and no disclosure of security failures is

171. In fact, an interesting symbiosis is emerging between white hat hackers and the FTC. White hats' tips on data leaks have in several instances directly resulted in subsequent FTC prosecutions of the entities. *See* Kevin Poulsen, *Petco Settles with FTC over Cybersecurity Gaffe*, SECURITYFOCUS, Nov. 17, 2004, http://www.securityfocus.com/news/9957.

172. Companies think that the current regulation is unclear and onerous. *See* Joseph Goedert, *HIPAA Compliance Strategies*, HEALTH DATA MGMT., July 26, 2002, at 33; *see also* Dean William Harvey & Amy White, *The Impact of Computer Security Regulation on American Companies*, 8 TEX. WESLEYAN L. REV. 505 (2002).

statutorily required,[173] the risk of prosecution remains low. Therefore, many entities do not view investing in security as a wise allocation of scarce corporate resources in the short term. Also, particularly for entities that are not in the technology sector, the requisite knowledge of information technology to construct more secure corporate information systems and processes is not necessarily available in-house. Hiring additional staff or obtaining the requisite security training for current staff will result in extra costs. In other words, the current legislative approach, which enables secrecy, arguably makes it more cost effective in the short-term for entities to make privacy promises that they are only somewhat concerned about breaching. It is also more cost effective to table investments in information security education and improvement until such time as the legal incentive structure changes.[174]

Further, "security through obscurity" hinges upon the idea that companies are capable of keeping secret information about vulnerabilities in their systems. However, this idea is critically erroneous because it greatly underestimates the technological skills of hackers. It also ignores the complexities of hacker culture; some hackers work as information security professionals by day and hack into systems by night or shift back and forth between the private sector and independent hacking.[175] However, disclosure of vulnerabilities is not always within entities' control. For example, some security breaches are perpetrated by hackers expressly for reputational and other nonpecuniary benefits; financial incentives are not necessarily involved. Therefore, hackers frequently openly discuss their exploits and the identities of vulnerable entities.[176] Consequently, even if the company attempts to prevent leakage of information regarding a penetration, it will not always be successful. Entities perpetually run the risk of negative reputational consequences because of a breach and the risk of other hackers replicating a breach.

---

173. Although COPPA, HIPAA, and GLBA require privacy statements, an entity's history of security gaffes and technological compliance with its stated privacy practices are not readily available in any centralized place for consumers to access. Most consumers will not know to look through the articles of Security Focus, the Register, or other information security trade press. *See* SecurityFocus, http://www.securityfocus.com (last visited Jan. 16, 2005).

174. This is not to assert that there are no individuals within business entities who care about information security. In reality, the opposite is frequently true. Conceptualizing a business entity as a single actor with a single voice and agenda does not accurately reflect the dynamic nature of corporate environments. However, security-conscious information technology professionals frequently have difficulty in internally selling the idea of allocating resources to corporate information security. The incentives for this investment are low in the short run under the current legislative approach and many other groups within such entities do not grasp the long term business benefits of good information security practices.

175. For an introduction to hacker culture, see The Mentor, The Conscience of a Hacker, http://www.insecure.org/stf/hacker_manifesto.html (last visited Jan. 17, 2005); DOUGLAS THOMAS, HACKER CULTURE (2002); Eric Steven Raymond, How to Become a Hacker, http://www.catb.org/~esr/faqs/hacker-howto.html (last visited Jan. 17, 2005).

176. Declan McCullagh, *Homeless Hacker Surrenders*, CNET, Sept. 9, 2003, http://news.com.com/2100-1009_3-5073426.html?part=msnbc-cnetCNET.

In the long run, of course, the calculus is (or should be) completely different. An entity's decision to short-change corporate information security is obviously undesirable in the long-term not only for society as a whole[177] but also for the entity itself. A critical component of an entity's strategy to maximize share value for the benefit of shareholders is protecting its proprietary information. Investing corporate resources into the development of new proprietary intangible assets without adequately protecting them reflects poor risk management planning and perhaps even corporate waste. The legal regime which encourages corporate secrecy through the "security through obscurity" model simultaneously encourages officers to erroneously focus on the short-term profit maximization in the area of information security strategy. A better legal paradigm is one which helps entities guide their own long-term information security planning; the current "security through obscurity" legislative approach fails on this front by encouraging secrecy rather than thoughtful risk management.

c. An Alternative Approach: "Security Through Process" and Kerckhoff's Law

The discussion above may seem to support the argument that imposing large fines on certain companies to make examples of them and striking fear in the hearts of other entities may be the best route to improving information security in the system as a whole. After all, if entities respond only to fear of liability then perhaps expectations and fears of liability should simply be generated. Impositions of liability for an egregious lack of care in information security may, in fact, be appropriate in some instances. However, even assuming that a critical mass of large awards and fines punishing the vulnerable will bring about the desired improvements in security, as a practical matter all judicial and regulatory proceedings take time, frequently years, from the point of filing to judgment. In the interim, the information security crisis will exponentially worsen. Therefore, simply relying on the development of this body of law is inadequate. If entities are not already moving toward the construction of more secure systems of their own volition, a stopgap measure is needed to incentivize improvements in corporate information security in the short-term while this body of information security case law develops.[178]

---

177. Conceptually, information security presents a type of short-term collective action problem: it is a case where entities have a choice between two alternatives and where, if they acted strictly rationally in the economic sense, the outcome would be worse for all, in their own estimation, than it would be if they were all to choose the other alternative. If every entity invested significant amounts of resources in information security in the short term, information crime would likely drop in the system as a whole. However, the financial incentives in the short term encourage entities to free-ride. Yet, the long-term benefits of information security improvements present an entirely different calculus. For a discussion of collective action problems, see JAMES COLEMAN, INDIVIDUAL INTERESTS AND COLLECTIVE ACTION: STUDIES IN RATIONALITY AND SOCIAL CHANGE (1986).

178. For example, a body of information security negligence case law is slowly emerging. *See* Foster *ex rel.* J.L. v. Hillcrest Baptist Med. Ctr., No. 10-02-143-CV, 2004 WL 254713 (Tex. App. Feb.

Perhaps our legal approaches should scaffold[179] entities in their development toward responsible information security risk management, thereby assisting them in learning how to hold themselves accountable to their shareholders for information security. Instead of endorsing "security through obscurity," our legal regime should endorse a paradigm where corporate accountability for information security to shareholders and society becomes part of regular process. This suggestion to shift from a legal model of "security through obscurity" to a paradigm of "security through process" mirrors the evolution of modern information security and cryptography theory. Modern information security and cryptography theory, having rejected "security through obscurity," embraces systems structured in line with Kerckhoff's Law.

Kerckhoff's Law asserts that the correct way to construct systems is to constantly test their security by assuming that almost all information about the system is public.[180] In other words, it is an "open" paradigm which is not predicated on total secrecy. It presumes that many different eyes are going to test the security of the system and that some of these "testers" may have skills as good as, or superior to, those of the creators of the security in the system. Therefore, almost complete disclosure of the operation of security in the system is presumed because attackers are assumed to be as astute as the technologists who constructed the security system.[181] Kerckhoff's Law, unlike "security through obscurity," correctly conceptualizes the severity of information risk from malicious third parties. Upon discovery of security holes which create vulnerabilities, the system evolves to correct for these holes, knowing that the holes will be quickly exploited again if not corrected. In other words, in this "security through process" model, security is conceptualized as an ongoing, relatively transparent and open process of construction, vetting, reconfiguration, and the correction of weaknesses in information security. Unlike "security through obscurity," "security through process" recognizes that no entity can maintain complete control over the knowledge of its information

---

11, 2004) (health data security breached by a medical center); *see also* Darcangelo v. Verizon Commc'ns, Inc., 292 F.3d 181 (4th Cir. 2002) (release of employee health data in connection with benefits plan administration); American Express Travel Related Servs., Inc. v. Symbiont Software Group, Inc., 837 So. 2d 434 (Fla. Dist. Ct. App. 2002), *rev. denied*, 851 So. 2d 729 (Fla. 2003) (customer financial information breached by a point-of-sale software manufacturer).

179. *See supra* note 12.

180. Bruce Schneier extends Kerckhoff to stand for the proposition that all security systems must be designed to fail as gracefully as possible. Kerckhoffs' principle applies beyond codes and ciphers to security systems in general: every secret creates a potential failure point. Secrecy, in other words, is a prime cause of brittleness—and therefore something likely to make a system prone to catastrophic collapse. Conversely, openness provides ductility. *See* Charles C. Mann, *Homeland Insecurity*, ATLANTIC MONTHLY, Sept. 1, 2002, at 81, *available at* http://www.theatlantic.com/doc/prem/200209/mann; *see also* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD (2000).

181. This rationale of openness forms the seminal theoretical underpinnings of the open source movement as well. *See* Eric Raymond, The Cathedral and the Bazaar, http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ (last visited Jan. 17, 2005).

security vulnerabilities.

A regulatory paradigm that mandates open dialog and creates a definitive legal process for the analysis of corporate information security risks, successes, and failures is superior. Corporate information security will not be compromised through openly discussing issues of information security management. Although entities may suffer from vulnerabilities in different ways, entities with strong information security practices tend to have much in common in the way they structure their systems. In fact, technologists in various entities frequently and openly discuss the information security challenges they face. However, discussions about these challenges within entities, particularly with legal departments and upper management, are few according to the PwC Study. Therefore, a regulatory approach that requires the participation of these groups of corporate decision makers outside the information technology department will stimulate internal corporate discourse on topics of information security. Similarly, a successful regulatory approach will encourage shareholders to hold officers accountable for prudent information security in the same manner that officers are accountable to shareholders, for example, for prudently managing the tangible assets of the entity. Improving information security is in the entities' own best interest; regulation can be used to help them to understand this interest and to compel them to realize that information security risks are risks that every entity faces.

A successful regulatory approach predicated on Kerckhoff's Law would require that entities set up an open process of disclosure and discourse of information security risks, failures, and successes, both internally and externally. Entities would shift away from a mindset of secrecy and a short-term cost-benefit security calculus toward a long-term perspective that views security as an ongoing, entity-wide process throughout the life of the entity. In particular, a successful regulatory approach will require that information security risk management be considered by the officers of the entity as a regular part of the strategic planning process. Such a regulatory approach may result in greater information security improvements in a shorter time frame than an approach that relies solely on entities' fear of liability. Similarly, because external reporting regarding information security practices would occur, ongoing oversight of information security management by both shareholders and appropriate agencies would become greatly simplified.

2. Scale-Free Networks and Information Security

Our current legal approach to information security lacks both adequate transparency and adequate consideration of the manner in which the properties of the transfer of information over networks impact information security

regulation. To this end, complexity theory[182] holds lessons for corporate law, generally, and for addressing the information security[183] crisis, specifically.[184] Regulation aimed at improving information security throughout a system must be crafted with an awareness of the system's organizational code,[185] the emerging dynamic structural properties of the system, and the impact of legal emergence on information security practices.[186] In other words, law and people

182. Complexity, in general, is the science examining the interrelationship, interaction and interconnectivity of various elements within a system and between a system and the environment in which it exists. The hallmarks of complex adaptive systems are distributed control, connectivity, co-evolution, sensitive dependence on initial conditions, emergent order, a state not in equilibrium, and a paradoxical condition of both order and chaos. *See* MITCHELL RESNICK, TURTLES, TERMITES AND TRAFFIC JAMS (1997); JOHN H. HOLLAND, HIDDEN ORDER: HOW ADAPTATION BUILDS COMPLEXITY (1995); Serena Chan, Complex Adaptive Systems, http://web.mit.edu/esd.83/www/notebook/Complex%20Adaptive%20Systems.pdf (last visited May 2, 2004). However, the exact contours of complexity theory vary from discipline to discipline. For an overview of twenty different views on complexity theory, see Joseph Sussman, Ideas on Complexity in Systems—Twenty Views, http://esd.mit.edu/WPS/esd-wp-2000-02.html (last visited Aug. 29, 2004).

183. The version of complexity espoused here may reject, in part, several key assumptions of traditional neoclassical economics, including the possibility of perfect information and the notion of corporations acting with a single rational voice. *See supra* note 93.

184. For various applications of complex systems theory to other legal contexts, see David G. Post & David R. Johnson, *"Chaos Prevailing on Every Continent": Toward a New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT L. REV. 1055 (1998) (arguing that legal theory would be enriched by paying attention to algorithms derived from the study of "complex adaptive systems" in contexts such as competitive federalism and the "patching" algorithm). *See also* Susan P. Crawford, *The Biology of the Broadcast Flag*, 25 HASTINGS COMM. & ENT. L.J. 603 (2003); Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 1 (2004); Robert A. Creo, *Mediation 2004: The Art and the Artist*, 108 PENN ST. L. REV. 1017 (2004); Jim Chen, *Webs of Life: Biodiversity Conservation as a Species of Information Policy*, 89 IOWA L. REV. 495 (2004); Scott H. Hughes, *Understanding Conflict in a Postmodern World*, 87 MARQ. L. REV. 681 (2004); Daniel A. Farber, *Probabilities Behaving Badly: Complexity Theory and Environmental Uncertainty*, 37 U.C. DAVIS L. REV. 145 (2003); Erica Beecher-Monas & Edgar Garcia-Rill, *Danger at the Edge of Chaos: Predicting Violent Behavior in a Post-Daubert World*, 24 CARDOZO L. REV. 1845 (2003); J.B. Ruhl & James Salzman, *Mozart and the Queen: The Problem of Regulatory Accretion in the Administrative State*, 91 GEO. L.J. 757 (2003); Daniel S. Goldberg, *And the Walls Came Tumbling Down: How Classical Scientific Fallacies Undermine the Validity of Textualism and Originalism*, 39 HOUS. L. REV. 463 (2002); Thomas R. McLean, *Application of Administrative Law to Health Care Reform: The Real Politik of Crossing the Quality Chasm*, 16 J.L. & HEALTH 65 (2001-02); James Salzman, J.B. Ruhl & Kai-Sheng Song, *Regulatory Traffic Jams*, 2 WYO. L. REV. 253 (2002); Jeffrey G. Miller, *Evolutionary Statutory Interpretation: Mr. Justice Scalia Meets Darwin*, 20 PACE L. REV. 409 (2000); Patricia A. Martin, *Bioethics and the Whole: Pluralism, Consensus, and the Transmutation of Bioethical Methods into Gold*, 27 J.L. MED. & ETHICS 316 (1999); J.B. Ruhl, *The Coevolution of Sustainable Development and Environmental Justice: Cooperation, Then Competition, Then Conflict*, 9 DUKE ENVTL. L. & POL'Y F. 161 (1999); Thomas Earl Geu, *Chaos, Complexity, and Coevolution: The Web of Law, Management Theory, and Law Related Services at the Millennium*, 66 TENN. L. REV. 137 (1998); Jeff L. Lewin, *The Genesis and Evolution of Legal Uncertainty and "Reasonable Medical Certainty,"* 57 MD. L. REV. 380 (1998); J.B. Ruhl, *The Fitness of Law: Using Complexity Theory to Describe the Evolution of Law and Society and Its Practical Meaning for Democracy*, 49 VAND. L. REV. 1407 (1996); Gerald Andrews Emison, *The Potential for Unconventional Progress: Complex Adaptive Systems and Environmental Quality Policy*, 7 DUKE ENVTL. L. & POL'Y F. 167 (1996).

185. For a discussion of what I call "architectures of growth," see Andrea M. Matwyshyn, *Mutually Assured Protection: Development of Relational Internet and Privacy Contracting Norms*, *in* SECURING PRIVACY IN THE INTERNET AGE (Margaret Radin et al. eds., 2005) (forthcoming 2006) (on file with author).

186. Legal emergence refers to the manner in which behavioral norms of various legal and business actors spontaneously self organize to form a dynamic organizational code that circumscribes future legal

do not exist in a vacuum; it is important to consider how the dynamic properties of information transfer in networks influences legal behaviors and their evolution. Applying this analytical lens of legal emergence[187] to the current regulatory paradigm, it becomes clear that current approaches to information security regulation erroneously adopt what might be termed a "clustering"[188] approach to controlling information transfer. Thus, the government has incorrectly conceptualized how to generate viral spread of good information security practices in the system and mitigate the transitive nature of information risk.

a. Rejecting a Clustering Approach

The current approach to information security, exemplified by statutes such as COPPA, HIPAA, and GLBA, attempts to regulate information security by creating legal "clusters" of entities based on the type of business they transact, the types of data they control, and that data's permitted and nonpermitted uses. In other words, the current regulatory approach has singled out a few points in the system for the creation of information security enclaves, points that engage in the transfer of children's data, health information,[189] and financial data.[190] Although addressing the particularly sensitive nature of these three kinds of data through regulation is a positive step toward improving the corporate information security of a few clusters of entities, it is by itself insufficient to improve information security in the system as a whole.

The current approach ignores the fundamental tenet of security that a system is only as strong as its weakest links, not its strongest points.[191]

---

strategies. Early theoretical discussion of spontaneous self ordering can be found in Hayek. *See* FRIEDRICH HAYEK, THE ROAD TO SERFDOM (1944). Law and legal norms are part of this web of mutual causation within a system, which I have elsewhere called "organizational code." For a discussion of organizational code, see Andrea M. Matwyshyn, *Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction Through Data Privacy*, 98 NW. U. L. REV. 493 (2004). Organizational code includes both market and nonmarket strategic decisions of actors within the complex adaptive system. For a discussion of nonmarket strategy, see S.L. Jarvenpaa & E.H. Tiller, *Integrating Market, Technology, and Policy Opportunities in E-Business Strategy*, 8 J. STRATEGIC INFO. SYS. 235 (1999).

187. Emergence, generally, is order that arises from the interactions of individual actors within a complex system, demonstrating a global pattern that could not have been forecast simply from understanding the behavior of one particular actor. *See* STEVEN JOHNSON, EMERGENCE: THE CONNECTED LIVES OF ANTS, BRAINS, CITIES AND SOFTWARE (2001).

188. For discussion of clustering behaviors in a complex system, see Cees van Leeuwen & Ionel Simionescu, *Robustness and Consistency of Dynamic Clustering of Complex Systems*, http://pdl.brain.riken.go.jp/publications/published/van_Leeuwen__Simionescu_Connection_Science_2002.pdf.

189. HIPAA restricts its scope to "covered" entities that handle personally identifiable health information, such as hospitals and insurance companies. Thus, not all sharing of health data necessarily falls under HIPAA.

190. GLBA addressed financial information held by "financial institutions" as defined by GLBA.

191. A security system is only as good as its weakest point. *See* Gary McGraw & John Viega, *The Chain Is Only as Strong as Its Weakest Link*, IBM DeveloperWorks, http://www-106.ibm.com/developerworks/linux/library/s-link.html (last visited Nov. 30, 2004).

Therefore, because this lowest common security denominator determines the security of the system as a whole, the better approach to controlling information throughout the system is to ensure that the least secure points in the system are strengthened and that the average level of security is as high as possible throughout the system. It will not prove adequate to only ensure that a few points or clusters in the system are particularly well-secured.

Also, much of information crime does not involve any of the data deemed particularly "sensitive" by the statutes at present. Many entities that aggregate large amounts of information do not fall into any of the categories of business entities currently regulated by information security statutes. The biggest economic losses arise not out of illegal leveraging of these protected categories of data; rather, losses arise out of stolen personally identifiable information, such as credit card data and social security numbers, which are warehoused frequently by entities that are not regulated by COPPA, HIPAA or GLBA. Therefore, creating enclaves of superior data security for data related to children online, some financial information, and some health data will not alleviate the weak information security in other parts of the system and will not substantially diminish information crime. Consequently, the goal of successful information security regulation will be to focus on the system as a whole and to expeditiously improve the weakest and average information security behaviors of all entities within the system, not merely that of clusters within the system.

b. Adopting a Focus on Transitive Closure, Hubs, and Nodes

The current regulatory approach also does not correctly consider the transitive nature of information risk. Defining risks associated with information security as *transitive* means that if an entity shares sensitive corporate information with a business partner and that partner experiences a data leakage that includes the shared data, the negative effects to the confidentiality and integrity of the data are similar to those that would have occurred if the original entity had been breached itself. Stated another way, each time an entity shares data, it takes a dependency on another entity. HIPAA and GLBA attempt to recognize this transitivity of risk by requiring that entities that share statutorily protected data contractually impose data care obligations on to their immediate trusted business partners. In this manner, stronger information security practices will presumably be transferred to the immediate business partners of entities subject to HIPAA and GLBA. These immediate business partners might be termed the "neighborhood" of an entity. In other words, the entire neighborhood of HIPAA and GLBA compliant entities adopts a stronger focus on information security.

Although this approach is a good starting point, the more appropriate scope

of encouraging a viral spread of security practices is the "transitive closure"[192] of entities rather than merely the entities' neighborhood. The transitive closure of an entity in the context of information security encompasses not only the added information risk from an entity's trusted partners but the also the risks from the partners of those partners and onward, following the chain of possession of the data end to end. The transitive closure of an entity is the proper scope of consideration and not the neighborhood. Even if an entity's immediate business partners maintain strong security in connection with shared data, if one of those business partners makes even one unwise outsourcing decision which gives access to the shared data to a third entity with weak security, the consequences of a data breach by this vulnerable entity two steps removed will be felt by the initial entity. The harm occurs regardless of the fact that the initial entity never directly chose the vulnerable entity as a business partner. Thus, the entire path of transfer of the data and the attendant risks must be included in the risk calculus; the transitive closure is the entire group of entities whose information security practices can impact the security of the data at issue.

Further, the current statutory framework inaccurately treats all entities that deal with particular types of data as an equal security risk to the system as a whole. Not all business entities within our economy are equal in size, success, or connectedness with the public or with other business entities; some entities are disproportionately more important to our economy as a whole than others. Thus, if the goal is to build a system of information security throughout the economy as quickly as possible, the best and most critical entities to enlist in improving security throughout the economy are those with the greatest number of connections to other entities and the largest transitive closures; the hubs of our economy.

This type of structure where some points in a system are more critical to the integrity of the system and more connected is a scale-free network.[193] In a scale-free network topology, a hub and node structure is visible where hubs are points connected to a significantly greater number of points than most others points, which are mere nodes.[194] Hubs are more stable than nodes, and their

192. Transitive closure refers to all points reachable from a particular point in a network, directly or indirectly, whose behavior impacts the behavior and risk profile of the initial point. *See* Robert Kozma, *Why Transitive Closure Is Important, available at* http://www.msci.memphis.edu/~kozmar/web-t_alg_n11-2.ppt.

193. A burgeoning literature in economics and the physical sciences discusses the structures of market and economic activity as demonstrating properties of scale-free networks. *See, e.g.*, Jan Matlis, *Scale-Free Networks*, http://www.computerworld.com/networkingtopics/networking/story/0,10801,75539,00.html; H.-J. Kim & I.-M. Kim, *Scale-Free Networks in Stock Markets*, 40 J. KOREAN PHYSICAL SOC'Y 1105 (2002), *available at* http://phya.snu.ac.kr/~kahng/econo.pdf; Diego Garlaschelli, Stefano Battiston, Maurizio Castri, Vito D.P. Servedio & Guido Caldarelli, *The Scale-Free Topology of Market Investments*, http://www.lps.ens.fr/~battiston/SF_TopoShareNets.pdf.

194. *See* THE STRUCTURE AND DYNAMICS OF COMPLEX NETWORKS (M.E.J. Newman et al. eds.,

elimination negatively impacts the survival of network as a whole to a greater degree than the elimination of a mere node. The way that information transfers most quickly in a scale-free network is through transmission from hubs[195] outwardly to nodes. Hubs have the greatest number of "edges" or connections with other points in the network; therefore more entities can be reached simultaneously. Infusing hubs results in transfer throughout the system more rapidly than it would from infusing a node. Similarly, because the transitive closure of hubs is generally larger than the transitive closure of nodes, the number of nodes that can be reached from a given point in the system is higher in the case of hubs.

It is fair to say that our securities laws and business realities have created a structure where publicly traded companies are the "hubs" of our economy. Publicly traded companies are most interconnected with other companies as well as with citizens in our society. As large entities, they frequently amass significant databases of consumer information which they can leverage in the marketplace while owing special duties to the public and their shareholders. Investors' and marketmakers' perceptions of public companies' corporate conduct are critical to the stability of stock markets and our economy. In addition, publicly traded companies tend to have more assets than private companies, and small entities frequently perceive doing business with a public company as a more attractive business choice than doing business with a private entity. Consequently, the most efficient manner of raising the level of information security within the network of our economy is through its hubs.

Therefore, the next part empirically explores the state of information security behaviors of the hubs of our economy, publicly traded companies, through annual reports, which are the primary communication mechanism with the market and shareholders. This inquiry aims to assess whether public companies have already adopted the "security through process" approach to information security. If they have done so, good information security practices are likely to begin virally spreading through the economy and revising current information security legislation to reflect a "security through process" paradigm may not be necessary as a practical matter. If meaningful disclosure of information security risks is occurring, it is likely that entities are successfully learning the importance of strong information security. Prudent entities will use the process of annual report filings to self-assess their practices and disclose the severity of the information security risks they face to their

2003); D.J. WATTS, SIX DEGREES: THE SCIENCE OF A CONNECTED AGE (2003); D.J. WATTS, SMALL WORLDS: THE DYNAMICS OF NETWORKS BETWEEN ORDER AND RANDOMNESS (1999).

195. For example, extensive work has been done on the spread of disease through social networks. *See* Christofer Edling & Fredrik Liljeros, *Social Contact Patterns and Disease Dynamics*, http://www.realinstitutoelcano.org/documentos/103/103.pdf.

shareholders.[196] If this type of disclosure is occurring, it is possible that good information security practices are already filtering through the system and perhaps no additional regulatory efforts are needed after all.

However, if no meaningful disclosure is occurring, it is likely that entities, like current legislation, are adopting the inferior paradigm of "security through obscurity." In other words, they are not adequately contemplating and risk managing the security of their systems. Unfortunately, this result is more in line with the findings of the PwC Study. As such, without the addition of a second layer to current regulation, good information security will not virally expand throughout the system, and inadequate corporate information security self-auditing and inadequate transparency mechanisms for external auditing will persist. Consequently, the information security crisis will also continue to worsen.

B. Assessing the "Hubs" Approach to Information Security: Corporate Information Security Disclosure Practices in 10K Filings

As discussed in the previous parts, Congress has statutorily articulated a social priority of stimulating more responsible corporate conduct in information security. This part undertakes an inquiry into what corporations are saying, or not saying, regarding the information security risks they face. Disclosures of information security practices by a publicly traded entity in its 10K filings, aside from being prudent risk management, also indicate adoption of a paradigm of "security through process." They further demonstrate that the entity is conscious of, and conducts analyses of the information security risks it faces. More broadly, in the aggregate, these disclosures speak to the extent to which improving information security is being incorporated into corporate behavior by the entities critical to the stability of our economy as a whole. The inquiry involved an empirical longitudinal analysis of 120 publicly traded companies' 10K annual securities filings across a five-year period. The analysis focuses on the dominant security paradigm adopted by the entities in the sample and the extent of information security disclosure occurring.

1. The Inquiry in Brief

A content analysis of the 10K filings of 120 publicly traded companies

196. Public companies would do so both to advise shareholders of the existence of security risks and to protect the entity from potential regulatory action by the SEC for failing to disclose what may be a material risk. Publicly traded entities are required to disclose material risks they face in their businesses as part of their securities reporting, in particular in annual 10K filings. For a discussion of risk factor disclosure, see, for example, Alan K. Austin & Steven V. Bernard, *Risk Factors Disclosure and the Private Securities Litigation Reform Act*, 1451 PLI/CORP 747 (Practising Law Institute—Corp. Law and Prac. Course Handbook Series, 2004).

from 1999, Time 1, and the most recent filing,[197] Time 2, was performed to examine the extent of information security risk disclosure and certain characteristics of each entity. Specifically, the level of information security disclosure of each entity in the sample was assessed in relation to whether each entity was a technology company; the novelty of the entity; the number of employees; whether the entity has a history of prosecution for security breaches; whether the entity has a publicized history of vulnerabilities; whether the entity's business is data intensive in nature; and the influence of prior information disclosure patterns.

The results of the inquiry demonstrated that less than half of the sample engaged in any information security disclosure in their 10K filings at Time 2. Increased information security disclosure at Time 2 tended to be associated with technology sector companies, companies with a history of prosecution, and companies which had disclosed information security risks at Time 1.

2. Hypotheses

It was hypothesized that:

Because of the greater likelihood of having in-house information security experts, entities in the technology sector would be more likely to understand the implications of information security vulnerability and, consequently, to engage in security disclosure at Time 2 than entities whose primary business is not technology related.

Newer entities will be more likely to disclose than older entities because they may be more attuned to the role of information systems in their enterprise.

Entities with more employees would be more likely to engage in security disclosure at Time 2 than entities with fewer employees because employees are a key source of information vulnerability.

Entities that have been prosecuted by the FTC or have defended against privacy suits would be more likely to engage in security disclosure than entities that have not been prosecuted or been defendants at Time 2.

Entities with a history of security vulnerability and data breaches would be more likely to engage in disclosure than entities without such a history at Time 2 because they may better understand the risks of information vulnerability than entities without a history of vulnerability.

Entities with data intensive businesses would be more likely to disclose information security risks than entities that are not data intensive because data intensive entities are more attractive information crime targets.

Entities engaging in information security disclosure at Time 1 will be more likely to engage in disclosure at Time 2.

197. As of August 2004.

3. Sample

The sample consisted of the 10K annual filings of 120 publicly traded companies[198] at two points in time, Time 1, 1999, and Time 2, each entity's most recent 10K. Specifically, the sample consisted of four groups of entities: (1) 30 entities that have either been prosecuted by the Federal Trade Commission for their privacy and security practices or have been the subject of civil class action suits from consumers on the basis of their privacy and security practices;[199] (2) 30 entities known to have suffered significant data security breaches but were not subject to FTC prosecution or consumer class action suit;[200] (3) 30 entities which have not been subject to FTC prosecution or consumer suit and have not suffered publicized significant data breaches, but are likely to be attractive targets for malicious actors in light of the consumer data intensive nature of the business;[201] and (4) a comparison group of entities which are not consumer data intensive and do not have a known history of data prosecution or vulnerability.[202]

---

198. Acxiom Corp.; Amazon.com Inc.; America West Holdings Corp.; AMR Corporation; American Express Co.; Wyeth; aQuantive.com, Inc.; Barnes and Noble, Inc.; Chase Manhattan Company; Choicepoint, Inc.; Delta Airlines, Inc.; DoubleClick Inc.; eBay Inc.; Eli Lilly and Company; Fleet National Bank; Guess, Inc.; Hershey Foods Corporation; Intuit Inc.; Looksmart Ltd.; Microsoft Corporation; Northwest Airlines, Inc.; Ohio Art Company; Pfizer, Inc.; Sabre Holdings; Time Warner Companies, Inc.; Toys "R" Us, Inc.; United Online, Inc.; Verizon Communications Inc.; Limited Brands, Inc.; Yahoo! Inc.; Agilent Technologies, Inc.; American Standard Companies Inc.; Baxter International; Cerner Corp.; Citrix Systems, Inc.; Coherent Inc.; Computer Network Technology; Computer Task Group Inc.; CSX Corporation; Electronic Data Systems Corp.; Digital Impact, Inc.; Eastman Kodak Co.; Electronic Arts, Inc.; Evans & Sutherland Computer Corp.; Gateway Inc.; Hanover International, Plc.; Harris Interactive Inc.; Hewlett-Packard Company; Hyperion Solutions Corporation; Intel Corporation; Keane Inc.; Kendle International Inc.; Merck & Co.; Polo Ralph Lauren Corporation; Procter and Gamble Company; Red Hat Inc.; Staples Inc.; Sybase Inc.; Walgreens Co.; WellMed, Inc.; Apple Computer, Inc.; AT&T Wireless Services, Inc.; Bank of America Corporation; Bank One Corporation; BJs Wholesale Club, Inc.; Cisco Systems, Inc.; CitiBank NA; Compaq Computer Corporation; Continental Airlines, Inc.; Morgan Stanley (Discover); Echostar Communications, Inc. (Dish Network); EarthLink, Inc.; e*Trade Financial Corporation; Ford Motor Credit Corp.; Gannett Co. Inc.; General Motors Acceptance Corporation; Ingram Micro Inc.; Interland, Inc.; International Business Machines Corporation; Knight-Ridder, Inc.; Lowe's Companies; MBNA Corporation; New York Times Co.; Oracle Corporation; Playboy Enterprises Inc.; PNC Financial Services Group, Inc.; Symantec, Corp.; U.S. Bancorp; Viacom, Inc.; Wells Fargo & Company; AK Steel Holding Corp.; Alcoa, Inc.; Ameron International Corporation; AptarGroup Inc.; Ball Corporation; Bemis Company, Inc.; Boise Cascade Corporation; Bowater Inc.; Carpenter Technology Corp.; Chesapeake Corporation; Commercial Metals Company; Crown Holdings Inc.; Deltic Timber Corporation; Eagle Materials, Inc.; Georgia Pacific Corporation; Lockheed Martin Corporation; Longview Fibre Co.; Louisiana Pacific Corporation; Masco Corporation; Nashua Corp.; Nucor Inc.; Oregon Steel Mills Inc.; Owens Illinois Inc.; PPG Industries Inc.; Quanex Corporation; Sherwin Williams Co.; Sonoco Producs Co.; Terex Corporation; Toro Company; United States Steel Corporation; Weyerhaeuser Co.

199. These entities were selected on the basis of information on the Federal Trade Commission website and Westlaw searches.

200. These entities were selected on the basis of press releases and articles located through searches using Google.

201. These entities were selected on the basis of their access to, collection and possible leveraging of protected categories of data as an integral part of their business—children's data, financial data, and health data.

202. These entities were selected on the basis of being manufacturing entities whose primary

4. Measures

a. Dependent Variable: Level of Disclosure at Time 2

Level of disclosure at Time 2 refers to the score of each entity in the sample on the Information Security Securities Disclosure Scale.[203]

b. Independent Variables

In this inquiry, the independent variables are technology business, business novelty, number of employees, data prosecution history, vulnerability history, data intensive business, and level of disclosure at Time 1.

i. Technology Business

Technology business refers to whether each entity in the sample is primarily an entity manufacturing or servicing information technology. It was operationalized as a dichotomous variable.

ii. Business Novelty

Business novelty refers the comparative newness of each corporate entity in the sample. It is operationalized as a continuous variable between 1900 and 2000, referring to the year the entity was first incorporated.

iii. Number of Employees

Number of employees refers to the number of employees most recently reported as employees of each entity in the sample.[204] It was operationalized as a continuous variable.

iv. Data Prosecution History

Data prosecution history refers to the presence or absence of a history of Federal Trade Commission actions against the entity for its handling of data security and a history of being named as a defendant in civil class action suits against the entity for data security-related harms. It was operationalized as a dichotomous variable.

---

products do not relate to information technology.

203. This scale was created by the author and consists of a scaled score of 0-8 which was tabulated by awarding one point for presence of each of the following possible disclosures: disclosure of a specific incident, disclosure of risks of government prosecution or civil suit arising out of privacy and security breaches, disclosure of risks of negative publicity from a security breach driving down stock price, disclosure of risks of malware, disclosure of risks of hacking, disclosure of risks of costs associated with industry custom changes, disclosure of risk of compliance costs and potential liability associated with additional regulation in the area of privacy and security, disclosure of other sources of other sources of vulnerability or costs associated with information security. Cronbach's Alpha was computed at .66 with 120 cases for the 2 items using the scale.

204. This information was collected from several sources including corporate websites and securities filings.

v. Data Vulnerability History

Data vulnerability history refers to the presence or absence of a history of publicized security breaches. It was operationalized as a dichotomous variable.

vi. Data Intensive Business

Data intensive refers to whether the primary business of the entity is contingent upon aggregation, storage, leveraging, or transportation of personally identifiable consumer data. It was operationalized as a dichotomous variable.

vii. Level of Disclosure at Time 1

Level of disclosure at Time 1 refers to the score of each entity in the sample on the Information Security Securities Disclosure Scale in its 10K filing from 1999.

5. Methodology

Each 10K filing at Time 1 and 2 was analyzed in terms of security vulnerability disclosure on the basis of the Information Security Securities Disclosure Scale,[205] and the "demographic" information about each entity for the variables of technology business, business novelty, number of employees, and data intensive business was obtained either from an entity's securities filings or from the entity's corporate website. Information regarding prosecution history was obtained from the FTC website and Westlaw. Data vulnerability history was obtained through Google. The resulting data was standardized and multiple regressions were performed. Multiple regression analysis was selected for analyzing the data collected in this study because it is a particularly potent method of quantitative analysis that facilitates identification of trends across many cases. In particular, multiple regression analysis provides the ability to disentangle the separate effects of independent variables while simultaneously assessing their correlation with one another.[206]

---

205. Each of the 240 10K filings was reviewed by two raters, with an interrater reliability result of 94.6%.

206. Multiple regression analysis and quantitative analysis generally have been critiqued as producing results which lack meaningful detail amidst expansive generality. Because a large number of cases are typically used in quantitative analyses, the particular dynamics of subsets of cases and particular cases are missing from the analysis. Similarly, the parsimony of variables that is valued in quantitative analyses has a cost: by explaining as much as possible with as few variables as possible, still more nuances of cases may be missing from the analysis. CHARLES C. RAGIN, CONSTRUCTING SOCIAL RESEARCH 132-35 (1994). Regression is a sufficiently powerful analytical tool to withstand a skewed sample. *See* Gerard E. Dallal, *Transformations in Linear Regression*, http://www.tufts.edu/~gdallal/regtrans.htm (last visited Mar. 20, 2006). Knowledge of general patterns regarding the information security disclosure practices of entities in this study may allow regulators to more effectively address the information security crisis. Because of the goals of this study, multiple regression analysis was an appropriate choice for analysis of the data.

Table 1. Level of Security Vulnerability Disclosure in 10K filings at Time 2

Hypothesis No.	1	2	3	4	5	6	7a	7b	7c
Tech company	.50***						.28***		.29***
	(.08)						(.09)		(.09)
Novelty		.32***					.05		.07
		(.09)					(.09)		(.09)
No. of employees			-.15*				-.08		-.09
			(.09)				(.08)		(.08)
Prosecution History				.29***				.11	.15*
				(.09)				(.09)	(.09)
Vulnerability History					.29***			.09	-.06
					(.09)			(.10)	(.10)
Data intensive						.29***	.08		.06
						(.09)	(.09)		(.10)
Disclosure Time 1							.39***	.50***	.36***
							(.08)	(.08)	(.08)
Constant	-4.81E-16	-5.27E-15	-3.40E-16	-3.41E-16	-2.25E-16	-6.94E-17	-1.25E-15	-4.55E-16	-1.51E-15
	(.08)	(.09)	(.09)	(.09)	(.09)	(.29)	(.08)	(.08)	(.07)
F	40.19	13.23	2.90	11.10	10.85	10.62	15.87	19.5	11.84
R^2(adj)	.25	.09	.02	.08	.08	.09	.38	.32	.39
N	120	120	120	120	120	120	120	120	120

*** significant at .10 level, p <.10**
**** significant at .05 level, p < .05**
***** significant at .01 level, p < .01**

Source: Author's compilation **Note: Standardized coefficients have been used.**

Ideally, the results obtained from this study will be replicated on a much larger scale. Thus, the goal is to identify tendencies present in individual publicly traded entities that will be germane to populations larger than the current population.

6. Results and Analysis

Overall, less than a half of the 120 entities in the sample engaged in any information security disclosures at Time 2. Therefore, widespread discussion of information security risks with shareholders is clearly not occurring. The results of regression analyses are discussed below and are presented in Table 1.

The question asked by Hypothesis 1, whether entities in the technology sector would be more likely to engage in security disclosure at Time 2 than entities whose primary business is not technology related, was answered positively. A regression analysis with disclosure at Time 2 as the dependent variable and technology companies as the independent variable yielded a significant difference in disclosure level at Time 2 at the .01 level of significance. Disclosure levels of technology entities in the sample were .50 of a standard deviation greater than the disclosure levels of non-technology entities.

Hypothesis 2 questioned whether newer entities tended to demonstrate higher levels of information security disclosure at Time 2. This question was

answered positively. The results obtained through performing regression analysis with disclosure level at Time 2 as the dependent variable and novelty as the independent variable and were statistically significant at the .01 level. For each increase of one standard deviation in novelty of the entity, disclosure at Time 2 increased .32 of a standard deviation.

Hypothesis 3 presented the question of whether a greater number of employees tends to coincide with increased disclosure levels at Time 2. The results of regressing disclosure level at Time 2 as the dependent variable and the number of employees as the independent variable at Time 2 generated significant results at the .10 level. However, counterintuitively, the greater the number of employees, the lower the level of disclosure of an entity tends to be. For each increase of one standard deviation in number of employees, the level of security disclosure of an entity at Time 2 decreased by .15 of a standard deviation.

Hypothesis 4 asked whether presence of a history of prosecution influences the extent of security disclosure at Time 2. Results of a regression with disclosure at Time 2 as the dependent variable and a history of prosecution as the independent variable generated revealed a positive impact of a history of prosecution on disclosure at Time 2 in the sample. Results were significant at the .01 level and showed that entities with a history of prosecution tended to demonstrate disclosure levels at Time 2 that were .29 of a standard deviation higher than entities without a history of prosecution.

Hypothesis 5 examined the influence of a history of information vulnerability on entities' disclosure practices at Time 2. Running a regression with disclosure level at Time 2 as the dependent variable and vulnerability history as the independent variable yielded a positive influence of vulnerability history on disclosure level. Disclosure at Time 2 of entities in the sample who were known to have a history of information vulnerability reflected levels that were .29 of a standard deviation higher than the levels of entities without vulnerability history. This result was significant at the .01 level.

The question asked by Hypothesis 6, whether entities with data intensive businesses at Time 2 are more likely to engage in vulnerability disclosure than entities that are not data intensive was answered positively. A statistically significant difference at the .01 level was found between the disclosure practices of entities with data intensive businesses and those of entities that do not operate inherently data intensive businesses. Data intensive entities' disclosure levels were .29 standard deviations greater than the disclosure levels of entities that did not have data intensive businesses in the sample.

Hypothesis 7 queried the impact of the entities' vulnerability disclosure at Time 1 as a predictor of the entities' disclosure level at Time 2. To wit, a series of three regressions produced varying results. First, a regression was conducted with disclosure level at Time 2 as the dependent variable and as the

independent variables, whether the entity was a technology company, the novelty of the company, the number of employees, and the data intensive nature of the business, controlling for disclosure level at Time 1. Technology entities reflected a .28 of a standard deviation higher disclosure score than non-technology entities in the sample at Time 2. This result was significant at the .01 level. Disclosure at Time 1 demonstrated a change of .39 of a standard deviation in disclosure at Time 2 for each change of one standard deviation of disclosure at Time 1. Meanwhile, controlling for novelty of the entity, number of employees, and the data intensive nature of the business of each entity in the sample yielded results that were not significant at the .15 level.

Second, a regression was conducted with disclosure at Time 2 as the dependent variable and data prosecution history and vulnerability history as the independent variables, controlling for disclosure at Time 1. Disclosure at Time 1 generated results significant at the .01 level of significance, with entities' tending to have a .50 of a standard deviation more positive disclosure at Time 2 in connection with a change of one standard deviation in disclosure at Time 1. No statistically significant result, measured at the .15 level of significance, was found in connection with a history of prosecution or vulnerability.

Finally, the "demographic" variables (technology entity, novelty, number of employees, data intensive business) were combined with the data history variables (prosecution history and vulnerability history) into one regression. A decrease of the effect of a one standard deviation change in disclosure at Time 1 resulted. Now a change of one standard deviation in disclosure at Time 1 was associated with a .36 of a standard deviation change in disclosure at Time 2. The result was significant at the .01 level. Prosecution history now increased in significance: a history of prosecution was associated with .15 of one standard deviation increased disclosure at Time 2. This was significant at the .10 level. Finally, a slight increase occurred for technology companies, now associated with disclosure levels at Time 2, which were .29 of a standard deviation higher than levels of non-technology companies. This result was significant at the .01 level and explained 39% of the variation in the dependent variable. This is a good fit.

7. Conclusion

Based on the results of the above regressions, it appears that the entities in the sample that engaged in disclosure at Time 2 tended to consist of technology companies, entities that had been prosecuted for data vulnerability, and entities with a history of disclosing security practices.

a. Corporate Information Security Learning is not Emerging Across Sectors in the Economy

Based on the existence of data privacy and security regulation, it would

have been expected that the data intensive nature of a business would coincide with higher levels of disclosure at Time 2, regardless of their prior disclosure practices. However, this was found not to be the case. Data intensive entities are not discussing the security risks they face and, therefore, tend not to create a feedback loop for external assessment of their data security processes and risks through disclosure. Instead, they appear to be adopting a paradigm of "security through obscurity." Apparently, entities with greater in-house technological expertise, i.e. technology companies, are more attune to the risks of information security and are disclosing accordingly. The difference in security disclosure levels between technology and non-technology entities in the sample can be explained in part by looking again to the theoretical concepts of first and second order change[207] and to the technology learning processes described in Part I(B).

First order change refers to learning how to do new things, while second order change refers to learning how to learn in new ways. An entity's collection and leveraging of data extensively in its business reflects first order change: the entity has learned to do something new as a consequence of the enabling power of technology. However, understanding information security and creating processes for addressing security within an entity reflects a second order change. Logically, technology entities, on average, start from a higher level of institutional technology knowledge than non-technology entities. As such, while non-technology entities are still developing in the first order stages of technology learning, technology entities can be presumed to have already progressed into the second order stage. Therefore, they may have a better understanding and mastery of controlling, leveraging, and protecting information assets and the security around them.

b. Corporate Information Security Learning is not Emerging Across Time Under the Prevalence of a "Security Through Obscurity" Paradigm

The companies in the sample that have historically disclosed security risks at Time 1 tended to continue to do so at Time 2, but apparently few additional companies are joining their ranks. This result tends to indicate that corporate security learning is not emerging in most entities across time. Alternatively, it could be argued that security learning may be emerging in non-technology entities but is simply not being disclosed. This theory would imply that entities have consciously adopted the suboptimal paradigm of "security through obscurity." Particularly when coupled with the PwC Study finding that advances in security are usually only in response to regulation and fear of liability, corporate information security learning is unlikely to be emerging. A majority of the sample has adopted the "security through obscurity" paradigm.

207. GREGEORY BATESON, STEPS TO ECOLOGY OF THE MIND 50 (1972).

Particularly in the case of non-technology entities, it is likely that entities do not understand the severity or the long-term implications of the information security risks they face. Consequently, it is also likely they are choosing to get the public relations benefits of making privacy promises and simply accepting the relatively low risk of prosecution.

c. Corporate Information Security Learning Appears to Emerge in Response to External Threat of Legal Audit and Sanction

The final significant result is that companies who have been prosecuted tend to engage in greater disclosure. The results of both the empirical inquiry in this article and the PwC Study indicate that entities invest greater resources in information security as a result of legal threat and not out of negative experiences with information vulnerability themselves. In the inquiry conducted in this part, entities prosecuted for data breaches engaged in better security disclosures than entities without a prosecution history. Meanwhile, entities with a history of vulnerability but without a prosecution history did not engage in better disclosure. Therefore, results seem to indicate that it is legal action which encourages self-assessment and disclosure.

These results may appear to advocate greatly increasing the frequency of prosecution for data security breaches. Although additional prosecutions may ultimately result in greater disclosure, fiscal realities of agency budgets make this suggestion a limited one in practice, in the short-term. Prosecution takes years in some instances, years during which the information security crisis will undoubtedly exponentially worsen. Prosecution also carries with it heavy administrative and legal costs not only for the prosecuting agency, but also for the entity being prosecuted. Arguably, this money is perhaps better allocated by the entity to improving security rather than defending regulatory action or civil suit. Similarly, the study described in this part did not evidence any clear "transitive" effects of prosecution—the entities disclosing information security risks tended to be the entities prosecuted themselves and not entities whose data intensive business models gave them reason to worry about vulnerability.

d. The Most Promising Approach to Improving Information Security is One Which Scaffolds the Emergence of Corporate Information Security Learning

The most promising approach for improving the security of information throughout the economy as quickly as possible rests in generating process-based feedback loops to allow for efficient assessment of entity conduct by regulators, marketmakers, shareholders, and consumers. Similarly, facilitating transitivity of good information security behaviors presents a critical part of adopting a "security through process" paradigm. Moving toward more secure systems is an ongoing process of learning to respond to ever-changing internal and external threats to security. A critical component is learning to address

information risk through, among other things, disclosure of failures and external assessment. This process does not appear to be meaningfully occurring for the entities in this sample.

The next part presents one possible means for leveraging existing securities regulation to generate feedback loops of disclosure of corporate information security behaviors. These feedback loops will result in three changes: (1) movement toward the information security and cryptography paradigm of "security through process" using securities law; (2) facilitating increased transparency of information for shareholders and marketmakers; and (3) scaffolding corporate learning of good security behaviors, which will be transferred onward to business partners and in time, may trickle down to consumers.

III. CREATING AN AUTOCATALYTIC SET OF INFORMATION SECURITY PROCESSES

This part proposes one method of moving toward improving the state of corporate information security in our economy through creating a legal autocatalytic set[208] of good corporate information security behaviors. [209] This approach is predicated on the information security and cryptography paradigm of "security through process," and informed by insights from complexity theory[210] about information transitivity in scale-free networks such as our

208. An autocatalytic set is a group of elements working together to generate a product that itself becomes the stimulus for the reaction which generates the next generation product. For a discussion of autocatalysis, see KAUFFMAN, *supra* note 14.

209. For discussions of the legal implications of information security, see Brenner, *supra* note 184 (arguing that the only successful approach to security is through a distributed security model); Thomas J. Smedinghoff, *The Developing Legal Standard for Information Security*, 796 PLI-PAT 465 (Practising Law Institute—Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, 2004) (setting forth the scope of prosecutions for computer security by federal agencies to date and providing business advice about structuring corporate security processes); Michael Rustad & Thomas Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77 (2003) (arguing tort law has failed to keep pace with online fraud and security issues); Ethan Preston & John Lofton, *Computer Security Publications: Information Economics, Shifting Liability and the First Amendment*, 24 WHITTIER L. REV. 71 (2002) (arguing that crafting a good liability regime for security publications must involve weighing not only the negative consequences of disclosure of a vulnerability but also the positive impact of preventing future exploitation of the vulnerability because of patching behaviors in response to its disclosure); Gary M. Schober, Shubha Ghosh, Ann Bartow, Chris Hoofnagle & Phyllis Borzi, *Colloquium on Privacy and Security*, 50 BUFF. L. REV. 703 (2002) (discussing the social impact of evolving technology on data control); Dean William Harvey & Amy White, *The Impact of Computer Security Regulation on American Companies*, 8 TEX. WESLEYAN L. REV. 505 (2002) (discussing the current state of corporate information security law in the U.S.); Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213 (1995) (arguing that the internet could quickly "veer into the highway to Hell" where "malefactors may cause a firm to unwittingly disclose its prime information commodities").

210. Complexity theory has been applied to analyze regulatory and social evolution in the context of environmental preservation and similarly presents a useful analytical lens for the present inquiry in Part III. For applications of complexity theory to environmental contexts, see Chen, *supra* note 184; Ruhl, *The Coevolution of Sustainable Development and Environmental Justice: Cooperation, Then Competition, Then Conflict*, *supra* note 184; Emison, *supra* note 184.

economy. Finally, the approach set forth in this part creates feedback loops reflecting the cybernetic elements of communication, control, and system.[211] Specifically, this part argues for adding line item disclosure requirements to Regulation S-K relating to information security and ensuring the certification procedures under the Sarbanes-Oxley Act include security auditing and analysis. Working to remedy the problem of information vulnerability in the economy falls squarely within the three-fold mission of the SEC—preservation of market stability, facilitation of capital creation, and investor protection. Securities laws provide an existing mechanism for encouraging the emergence of good information security behaviors in the "hub" entities of our economy, publicly traded entities. Leveraging existing successful regulatory frameworks and legal mechanisms provides a more efficient approach than starting over through new data control legislation.

A. Crafting Legal Autocatalytic Sets

When scientists speak of *autocatalytic sets*, they refer to collections of elements where the product of the initial reaction of combining the elements will act as a catalyst for the creation of other reactions of the set. In other words, the product and reactions of the set of elements will be able to self-sustain.[212] It is this type of reaction chain which effective legal regulation initiates.

An effective legal regime will generate an autocatalytic set that commences the process of legal emergence of norms, behaviors, and structures that enable continued economic growth; elsewhere called the "architectures of growth."[213] A change in corporate security behavior, though initially instigated in response to law, can become a self-sustaining autocatalytic set of good information security behaviors. In other words, the product of legal compliance will itself stimulate better information security behaviors in the future.

It is this type of autocatalytic set of information security behaviors that the following part attempts to introduce. The narrow additions to securities law proposed in the next part attempt to assist entities in implementing a paradigm of "security through process" within their operations in a self-sustaining manner. Entities will also become more sensitive to the dangers their business partners pose to information security compromise. Consequently, entities will begin to contractually require good security behaviors from them, another self-sustaining mechanism for virally spreading good security behaviors through the system.

---

211. *See supra* note 13.

212. *See* KAUFFMAN, *supra* note 14.

213. *See* Matwyshyn, *supra* note 185. Architectures of growth are emergent legal constructions that facilitate commercial development.

Simultaneously, the proposals below begin to introduce greater transparency into information security behaviors of corporate entities. This will assist shareholders and marketmakers in receiving accurate information regarding corporate security practices—information that should be reflected in stock price, and therefore generating another self-sustaining mechanism for monitoring care in corporate information security. Finally, perhaps the last self-sustaining behaviors may arise from the positive externalities of entities educating their employees in handling corporate information in a careful manner. Some of these lessons of good security practices may be transferable to these employees' own consumer security behaviors and practices outside the workplace or may at least raise consumer awareness of information security threats.

B. Feedback Loops Through Cybernetics and Securities Law

Autocatalytic sets usually involve creation of critical feedback loops. In order to allow systems to develop in a manner which improves performance, three elements comprising feedback loops are necessary—communication, control, and system.

1. Communication

Adequate communication for building an information security feedback loop within our economy must start with finding the weakest points in the network. To accomplish this, enough security information must be available to enable identification of particularly vulnerable "hub" entities in our economy. Requiring that entities keep track of, and analyze, their annual losses arising out of various types of information security breaches will instigate a process of more careful information security monitoring. This process of data security loss analysis will help entities understand their own weaknesses and will allow for identification of entities whose information security practices seem to lack improvement and disproportionately burden the system. Specifically, this part argues for improving communication by using existing securities laws[214] to mandate line-item disclosure of information security losses through, for example, expanded Items 103 (legal proceedings), 303 (MD&A), and 308 (internal controls) of Regulation SK. Similarly, leveraging Section 404 of the Sarbanes-Oxley Act, certification of audit procedures and financial statements, should demonstrably take into account issues of information security.

214. For a discussion of the evolution of securities laws in response to technology, see Roberta S. Karmel, *Regulatory Initiatives and the Internet: A New Era of Oversight for the Securities and Exchange Commission*, 5 N.Y.U. J. LEGIS. & PUB. POL'Y 33 (2001-02).

a. Creating Feedback and Transparency: Regulation S-K [215] and Sarbanes-Oxley ("Sarbox")

Although Congress is increasingly allocating attention to data control legislation,[216] it appears that entities and consumers[217] have not yet grasped the importance of information security. Business entities underestimate the severity of financial losses that result directly and indirectly from weak information security practices. As demonstrated by the empirical inquiry in Part II, entities tend not to consider the information risks they face to be "material" or detrimental to their financial integrity.[218] Part of the reason for this knowledge deficit may pertain to the absence of feedback loops relating to information security in the system.

One manner of creating a feedback loop, which appeared to be effective in the empirical inquiry in Part II, is through litigation. In theory, a feedback loop could be judicially created by deeming information security disclosures to be "material" disclosures that all publicly traded entities should be including in their disclosure statements. Unfortunately, however, relying on courts to craft such a doctrine of "materiality" that encompasses disclosures of information security information will be a quixotic course of action. The materiality standard has been a hopeless morass of disparate caselaw for decades.[219]

---

215. REG. S-K, 17 C.F.R. § 229.101, *available at* http://www.sec.gov/divisions/corpfin/forms/regsk.htm#des.

216. Outside of the United States, governments are also paying attention to information security issues. The approach to data privacy adopted by the United States is less stringent than that adopted by the member states of European Union and Canada. *See* Gant Goss, Spam Agreement Between U.S. and E.U. May Be on the Way, ITWORLD, July 17, 2003, http://www.itworld.com/Man/2695/030717spamagreement/.

217. *But see* Richard Trinkner & Brian Smith, *Consumer Technology Adoption Roadmap*, http://www.gartnerg2.com/site/FileStream.asp?SID=0&File=wp-0902-0002.pdf (discussing quickening pace of consumer adoption of technology).

218. As part of 10K annual reports, public entities are required to disclose all "material" events in the life of the business that may impact a shareholder's investment in the entity. The definition of materiality, however, is in flux and much discretion regarding whether an event is "material" for disclosure purposes remains with the company engaging in the disclosures. For a discussion of materiality, see Yvonne Ching Ling Lee, *The Elusive Concept of "Materiality" Under U.S. Federal Securities Laws*, 40 WILLAMETTE L. REV. 661 (2004); Patrick Hall, *The Plight of the Private Securities Litigation Reform Act in the Post-Enron Era: The Ninth Circuit's Interpretation of Materiality in Employer-Teamster v. America West*, 2004 BYU L. REV. 863; Hugh Beck, *Determining the Materiality of Earnings Forecasts Under the Private Securities Litigation Reform Act in Helwig v. Vencor*, 2002 BYU L. REV. 111; Nicholas Kappas, *A Question of Materiality: Why the Securities and Exchange Commission's Regulation Fair Disclosure Is Unconstitutionally Vague*, 45 N.Y.L. SCH. L. REV. 651 (1990); John M. Newman, Jr., Mark Herrmann, & Geoffrey J. Ritts, *Basic Truths: The Implications of the Fraud-on-the-Market Theory for Evaluating the "Misleading" and "Materiality" Elements of Securities Fraud Claims*, 20 J. CORP. L. 571 (1995); Alan J. Rubenstein, *Basic, Inc. v. Levinson: Materiality of Preliminary Merger Negotiations and the Presumption of Reliance Under Rule 10b-5 of the 1934 Securities Exchange Act*, 2 DEPAUL BUS. L.J. 331 (1990).

219. Materiality has been defined differently in different securities law contexts by courts. In some instances a "probability-magnitude" test is applied by courts. *See, e.g.*, Basic v. Levenson, 485 U.S. 224 (1988). Materiality is determined by whether the magnitude of the potential loss is so great that even a remote risk required disclosure or provides basis for actions for fraud under Section 10b5. *See, e.g.*, SEC v. Texas Gulf Sulphur Co., 401 F.2d 833, 867 (2d Cir. 1968) (en banc), *cert. denied*, 394 U.S. 976

Therefore, a more promising method of generating a feedback loop is by adding a new line item disclosure requirement or expanding existing line item disclosures in Regulation S-K. Regulation S-K sets forth the requirements that information entities must disclose in their quarterly 10Q and annual 10K filings.[220] At least three sections lend themselves to expansion with additional information security specific disclosure requirements: Items 103, 303, and 308.

i. Regulation S-K, Item 103—Legal Proceedings

Item 103 requires that entities disclose "material pending legal proceedings other than ordinary routine litigation incidental to the business,"[221] and, in particular, must disclose any proceeding which relates to a discharge of materials into the environment where a governmental authority is a party and the entity believes that monetary sanctions resulting will be more than $100,000.[222] Just as this special carveout was created by the SEC for environmental losses,[223] a new special carveout can be created for information security losses. However, because of the unique nature of information security harms, information security-related regulatory action should be exclusively carved out from the definition of "ordinary routine litigation" in Item 103.

The harms of information vulnerability, unlike a toxic landfill, are not geographically localized or containable; information, once obtained, can be resold and used by numerous individuals concurrently to cause harm. A breach of security, which carries a small regulatory fine, may occasion systemic damage and corporate losses far in excess of the amount of the fine. More

---

(1969). The SEC then adopted this same standard of materiality in an SEC Enforcement Release and 1988 SEC interpretive release for MD&A disclosures. *See In re* American Sav. & Loan Ass'n of Fla., Exch. Act. Rel. No. 34-25788 (June 8, 1988); Exch. Act. Rel. No. 34-25951 (Aug. 3, 1988). Then, in a 1989 MD&A release, the SEC explicitly stated that MD&A materiality standards differ from those adopted in *Texas Gulf Sulphur*. This 1989 Release instructed management to make two assessments to determine materiality: (1) whether the particular trend, event or uncertainty is reasonably likely to happen and (2) if management cannot determine the likelihood of occurrence, then evaluate the contingency on the assumption that it will happen. Exch. Act. Rel. No. 34-26831 (May 18, 1989).

An altogether different definition appears in insider trading contexts. Information is material for purposes of creating the basis of an insider trading action if "there is a substantial likelihood that a reasonable shareholder would consider it important" in deciding how to act. *See* TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976). In the long term, the materiality standard for disclosure should be doctrinally reconciled in favor of a reasonable investor standard that dovetails with standards of "reasonableness" in other areas of law, particularly tort law. For a discussion of the historical evolution of consumer protection standards and tort law, see MARSHALL SHAPO & PAGE KEATON, PRODUCTS & THE CONSUMER: DECEPTIVE PRACTICES (1972); MARSHALL SHAPO & PAGE KEATON, PRODUCTS & THE CONSUMER: DEFECTIVE & DANGEROUS PRODUCTS (1970). Information security negligence claims will result in a construction of "reasonable" security practices, "reasonable" corporate conduct in contracting, and "reasonable" users. In the interim while awaiting such a doctrinal movement, the Securities and Exchange Commission can work to educate both businesses and investors about the importance of information security through mandating particularized disclosure.

220. 17 C.F.R. § 229.1 (2005).

221. § 229.103.

222. Instructions to 17 C.F.R. § 229.103.

223. *See infra* note 248.

importantly, if an entity is so vulnerable that a regulatory agency is willing to allocate resources for its prosecution, this entity should be flagged in the market as weakly protecting its intangible assets. Information vulnerability within an entity is rarely a localized problem; it generally indicates a problem of inadequate security throughout the entity. Similarly, any class action litigation related to information security, particularly information security negligence, should be disclosed and not deemed litigation in the ordinary course of business.

ii. Regulation S-K, Item 303—Management Discussion and Analysis ("MD&A")

One of the central requirements of Form 10K is the section entitled Management Discussion and Analysis of Financial Condition and Results of Operations or "MD&A."[224] The goal of this section is to enable investors to analyze the financial health, culture, goals, and identity of the corporation from management's perspective. Therefore, the section is intended to include discussion of trends, unusual or important events and corporate risks that are likely to materially impact the company.[225] MD&A disclosures[226] complement "risk factor" disclosure in registration statements under the 1933 Securities Act and form an increasingly integral part of periodic reporting under the 1934 Exchange Act.[227] Most recently, the passage of Sarbanes-Oxley ("Sarbox") and new rules promulgated under it also enlarged the scope of the discussion required in MD&A.[228]

---

224. Requirements are set forth in Item 303 of Regulation S-K. "The MD&A requirements are intended to provide, in one section of a filing, material historical and prospective textual disclosure enabling investors and other users to assess the financial condition and results of operations of the registrant, with particular emphasis on the registrant's prospects for the future." Exch. Act Rel. No. 33-6835 (May 24, 1989). Regulation S-K, Item 303(a) sets forth the general MD&A requirements applicable to full fiscal years. It states that: "[t]he discussion shall provide information as specified in paragraphs (a)(1) through (5) of this Item and shall also provide such other information that the registrant believes to be necessary to an understanding of its financial condition, changes in financial condition and results of operations." *See also* MD&A Proposal & 2003 MD&A Guidance, http://www.sec.gov/rules/proposed/33-8098.htm (emphasizing that MD&A "should not be merely a recitation of the financial statements in narrative form or an otherwise uninformative series of technical responses to MD&A requirements, neither of which provides the important management perspective called for by MD&A" and emphasizing that MD&A also requires "analysis" as well as "discussion").

225. 17 C.F.R. § 229.303(a)(3)(i) requires disclosure of "known trends or uncertainties that have had or that the registrant reasonably expects will have a material favorable or unfavorable impact" on future income.

226. "The Commission has long recognized the need for a narrative explanation of the financial statements, because a numerical presentation and brief accompanying footnotes alone may be insufficient for an investor to judge the quality of earnings and the likelihood that past performance is indicative of future performance. MD&A is intended to give the investor an opportunity to look at the company through the eyes of management by providing both a short and long-term analysis of the business of the company. The Item asks management to discuss the dynamics of the business and to analyze the financials." Exch. Act Rel. No. 33-6711 (Apr. 24, 1987).

227. *Id.*

228. Also, in December 2003, the SEC issued Release 34-48960 regarding preparation of MD&A.

Item 303 can be expanded to include paragraph (a)(6), which specifically addresses information security strategy and failures that have, or are reasonably likely to have, a current or future effect on a company's financial condition, revenues, or expenses;[229] particularly, intangible assets protected principally through trade secret law.[230] This new requirement can be crafted to mirror the recent addition of paragraph (a)(4) to Item 303, which directly addresses off-balance sheet arrangements and was added on January 27, 2003 in the wake of the Enron collapse.[231] Particularly in light of the SEC's recent move to make filings more readily analyzable with software applications,[232] a new disclosure requirement would enable monitoring of entities with weak information security. If these initiatives that require companies to file periodic filings in machine-readable format succeed, analysis of security behaviors over time would be an easily accomplished task with the assistance of software. Therefore, mapping the most vulnerable points among the hubs of our information economy will be an easily surmountable task that will save U.S. corporations billions of dollars in the aggregate in information security-related losses annually.

Also, just as in the context of disclosure under Item 303 with regard to

---

In this manner and through enforcement actions, the SEC is signaling its increased attention to MD&A compliance. SEC pronouncements on MD&A and qualitative disclosure have included the following: 1980 - SEC adopts present disclosure requirements for MD&A (Release 33-6231); 1981 - SEC issues staff interpretive guidance for MD&A (Release 33-6349); 1987 - Public comment sought on adequacy of MD&A and on proposed revisions (Release 33-6711); 1989 - SEC issues staff interpretive release MD&A (Release 33-6835); 1999 - Segment Information – Release 337620, which adopted technical amendments to conform the reporting requirements with FAS No. 131 so that narrative disclosure in reports must relate to each operating segment when segment financial reporting is required; 2001 - Release 33-8040 discusses a review of Fortune 500 annual reports results in comment letters, many of which commented on MD&A to more than 350 of these companies. Cautionary advice is issued encouraging companies to include in MD&A full explanations of their "critical accounting policies;" 2002 - SEC issues interpretive guidance for MD&A (Release 33-8056) and SEC proposes additional MD&A disclosure requirements for critical accounting estimates (Release 33-8098); 2003 - Additional MD&A disclosure requirements adopted for off-balance sheet arrangements and contractual obligations (Release 33-8182) and SEC issues guidance on MD&A (Release 33-8350).

229. Setting forth a minimum dollar amount in the line item may be a prudent idea to avoid a portion of the conflicts that plague the evolution of materiality doctrine. One approach for setting this minimum dollar amount may be to track the levels specified in the Computer Fraud and Abuse Act (18 U.S.C. § 1030) regarding what level of damages must be shown to bring a prosecution.

230. Employees are a primary source of trade secret and information security compromise. *See, e.g.*, Jane Howard-Martin, *Companies, Employees Fight for Trade Secrets*, USA TODAY, Dec. 18, 2002. Frequently an initial line of defense to an allegation against a former employee of stealing trade secrets is demonstrating that adequate information control practices were not in place in an entity and hence, material in question was not a trade secret.

231. *See* Exch. Act Rel. No. 33-8182. Recently added paragraph (a)(5) requiring disclosure of contractual obligations could be also be expanded to include as a required disclosure category contracts that involve the number of parties with which the entity shares consumer personally identifiable information. Through this addition of contractual consumer datasharing category, networks of data sharing can be mapped and the sources of information vulnerability more readily realized, a important capability because any vulnerability in the information system negatively impacts the system as a whole and entities unrelated to the initial data leakage.

232. *See* Securities & Exchange Commission, Concept Release, Exchanging Commission Data Through Tagged Files (2004), http://www.sec.gov/rules/concept/33-8497.htm.

compliance with Federal, State, and local provisions regulating discharge of materials in the environment,[233] entities should report the extent of capital expenditures they were forced to undergo, or will be forced to undergo, for the remainder of the current fiscal year and the succeeding fiscal year, or such longer period the registrant deems relevant, to comply with new privacy and security legislation. By reporting these numbers, the cost effectiveness of new legal approaches to data control can be more easily assessed. Reporting these expenses also provides the entity a benefit in litigation by generating a record of efforts at exercising "due care" in maintaining information security. This record of care can become critical evidence for defense in information security negligence actions.

iii. Regulation S-K, Item 308—Internal Controls

The frameworks used by entities to assess integrity of financial reporting should consider information security and integrity as part of their structure. Item 308 of Regulation S-K requires that management provide a report on internal controls over financial reporting, including identifying the framework used for analysis of effectiveness of controls and an attestation regarding the level of efficacy of existing internal controls. Item 308(a)(3), which already requires that management disclose any material weakness in internal controls over financial reporting,[234] can be expanded to specifically carve out information security breaches as one type of material weakness that must be disclosed under this item. In particular, information security audits, such as SAS 70 audits,[235] should be a regular part of operations assessment that 308(a)(2) requires to be noted as a means of assessment of current internal controls. If an entity experiences repeated data vulnerabilities, particularly serious intrusions by third parties into the entity's information systems, it is

233. Item 303 (xii) states that "[a]ppropriate disclosure also shall be made as to the material effects that compliance with Federal, State and local provisions which have been enacted or adopted regulating the discharge of materials into the environment, or otherwise relating to the protection of the environment, may have upon the capital expenditures, earnings and competitive position of the registrant and its subsidiaries. The registrant shall disclose any material estimated capital expenditures for environmental control facilities for the remainder of its current fiscal year and its succeeding fiscal year and for such further periods as the registrant may deem material." *But see* Request for Rulemaking for Clarification of Material Disclosures with Respect to Financially Significant Environmental Liabilities and Compliance with Existing Material Financial Disclosures, http://www.sec.gov/rules/petitions/petn4-463.htm (discussing confusion in the environmental materiality standards); Comments on Rulemaking Petition: Clarification of Material Disclosures with Respect to Financially Significant Environmental Liabilities and Compliance with Existing Material Financial Disclosures, http://www.sec.gov/rules/petitions/4-463.shtml. For a discussion of environmental disclosure requirements under securities laws, see Richard M. Shwartz & Donna Mussio, *Environmental Disclosure Requirements Under the Federal Securities Laws*, 1424 PLI-CORP 333 (Practising Law Institute—Corp. Law and Prac. Course Handbook Series, 2004).

234. 17 C.F.R. §§ 229, 308(a)(4) (2005).

235. SAS 70 audits pertain to an in-depth audit of a service organization's control activities, which generally include an inspection of controls over information technology and other security processes. *See* About SAS70, http://www.sas70.com/about.htm.

possible that the integrity of the financial auditing processes has been corrupted and attestation of integrity may be improper. Similarly, an entity must consider the extent of the diminished value of compromised data and its impact on reporting intangible asset values on financial statements.

iv. Sarbox, Section 404—Officer Certification of Internal Controls

Sarbox addresses the accuracy of audit processes and the security of corporate information of publicly traded entities. Particularly, section 404 requires that entities establish adequate internal controls and auditing procedures[236] certified by management[237] regarding the financial statements of the entity.[238] Consequently, information security is reflected in two ways in Sarbox. First, entities are required to establish information security processes and audit procedures to protect against information vulnerability. Second, entities must accurately reflect the diminished value of any intangible assets compromised as a result of information security breaches on their financial statements. In other words, information regarding the value of intangible assets, which includes both consumer information and trade secret information, must be accurately reported. If the data has been compromised, the reported value must reflect this negative change in value, just as discussed above in the context of Item 308 of Regulation S-K.

Because Section 302 of Sarbox specifically authorizes the SEC to promulgate rules regarding officers' responsibility to certify the accuracy of financial statements and auditing process,[239] the SEC is authorized to promulgate a rule specific to information security reporting and certification in connection with Section 404 of Sarbox. As part of this new certification rule regarding information security, the SEC should require attestation that any providers and business partners (and the partners of those partners, down the entire length of the chain of data transfer) receiving data from the entity are under contractual obligations to maintain security of the data shared in accordance with law and privacy promised otherwise made by the entity to consumers. Thus, truthful attestation of data control imposes an obligation on publicly traded entities to require care in information security both from themselves and from all other subsequent entities that come into contact with an entity's data.

---

236. For example, one auditing procedure that specifically relates to information security is an SAS70 audit. *Id.*

237. Section 302 authorized the SEC to promulgate rules regarding officers' responsibility to certify the accuracy of financial statements and auditing procedures. *See* Final Rule, Certification of Disclosure in Companies' Quarterly and Annual Reports, 17 C.F.R. pts. 228, 229, 232, 240, 249, 270 & 274, *available at* http://www.sec.gov/rules/final/33-8124.htm [hereinafter *Final Rule*].

238. 107 P.L. 204, § 404.

239. *See Final Rule*, *supra* note 237.

b. Creating Transitivity of Good Information Security Behaviors

As described above, additional information security disclosure requirements under securities laws will facilitate greater transparency in corporate information security behaviors on an ongoing basis. In this manner, it will bring about a shift in the regulatory paradigm to "security through process." Additional disclosure requirements will also assist in disseminating good security throughout the system. They will create transitive effects and viral spread of good information security behaviors throughout the transitive closure of the public company or "hub" throughout the system.

As previously discussed, data risk within the transitive closure of the hub is assumed by the hub as a breach at any point in the data sharing chain impacts the hub. Therefore, public entities are responsible not only for the integrity of their information and internal operations but also for remotely connected nodes in their transitive closure. Thus, an explicit requirement that public entities must certify the information security practices of all entities within their transitive closure ensures both greater information integrity and greater transitivity of good information security behaviors. A hub can contractually insulate itself by creating a group of nodes directly and indirectly around it that demonstrate certain minimum levels of data care. In other words, public entities that engage third parties to provide services in data processing, storage, conveyance, or leveraging of corporate information will be required to contractually impose on these business partners both a duty to maintain basic levels of information security and a duty to ensure security in onward transfer.

Through contractual imposition of good security behavior obligations on all entities within the transitive closure of the publicly traded entity, the system will quickly disseminate improved information security norms. In this manner, nodes doing business with a hub will improve information security practices within their entities to maintain the business relationship with the hub and, in turn, require their business partners to do likewise. These improved security behaviors may then become standard practice throughout the system and set a new business norm.

2. Control

In the context of the new communication mechanisms proposed in this part, two principle control benefits will result. First, these additional disclosures will better allow shareholders of an entity to overcome the agency problem often discussed by corporate law scholars,[240] enabling better shareholder oversight of

240. *See, e.g.*, ADOLF A. BERLE & GARDINER C. MEANS, THE MODERN CORPORATION AND PRIVATE PROPERTY 2-5 (1935). For a discussion of Berle and Means, see William W. Bratton, *Berle & Means Reconsidered at the Century's Turn*, 26 J. CORP. L. 737 (2001). *See also* Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure*, *in* FOUNDATIONS OF CORPORATE LAW 7 (Roberta Romano ed., 1993); Stephen M.

corporate activity. Similarly, marketmakers will gain better access to information about information security breaches in order to ensure that corporate information vulnerability, security losses and diminution of intangible asset value are being factored into stock price of vulnerable entities. Under the status quo, this information may not currently be reaching marketmakers in a timely manner.

Through additional disclosure requirements, part of the collective action problem inherent in corporate information security investment will be remedied. Currently, one of the business drivers that keep some entities from investing in security is the unwillingness to be the first-mover in raising security standards; if competitors are not investing in security, it may seem imprudent or extravagant to do so. However, a uniform disclosure requirement would reframe the decision, changing good security from a luxury to an essential business expense that must be incurred by all entities. This new corporate focus on better security, in turn, will result in long-term value creation for the entities themselves both directly and indirectly.

a. Eliminating the Corporate Agency Problem with Regard to Information Security Losses and Strengthening Shareholder Control over Corporate Information Security

One of the key elements of the "security through process" paradigm is the expectation that third parties will be able to find vulnerabilities in an entity's information security systems. In this manner, external accountability is layered onto an entity's internal accountability processes for vulnerabilities. In other words, control over security becomes shared between the entity and the imagined community[241] of its external security auditors.[242] As a consequence, vulnerabilities are taken more seriously and cannot be ignored in the way that a "security through obscurity" paradigm allows.

This structure mirrors the mechanisms of shareholder control in a corporation. In a corporation, one of the initial and most important sources of external auditing is shareholder scrutiny. Corporate law theory frequently

---

Bainbridge, *The Politics of Corporate Governance*, 18 HARV. J.L. & PUB. POL'Y 671, 672 (1995) (noting that modern scholars refer to the Berle and Means problem as an agency problem); Adolf A. Berle, *For Whom Corporate Managers Are Trustees: A Note*, 45 HARV. L. REV. 1365 (1931) (arguing that corporations exist exclusively to make profits for the shareholders).

241. For a discussion of "imagined communities," see BENEDICT ANDERSON, IMAGINED COMMUNITIES (1983).

242. For an example of norms developing in the whitehat hacker/security researcher community with regard to reporting security vulnerabilities, see Rain Forest Puppy, Full Disclosure Policy (RFPolicy 2.0), http://www.wiretrip.net/rfp/policy.html. For discussion of the benefits and costs of including whitehats and blackhats in monitoring, see Michelle Delio, *Bug Finders: Should They Be Paid?*, WIRED NEWS, Aug. 9, 2002, http://www.wired.com/news/technology/0,1282,54450,00.html; Brent Wible, *A Site Where Hackers Are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime*, 112 YALE L.J. 1577 (2003).

contemplates issues of the agency problem of shareholders' suboptimal inclusion in the decision-making processes of the entities they own.[243] Because of this agency problem, shareholders can be limited in the information they receive and are consequently unable to act as a check on corrupt or adverse actions of officers and directors.

Management of an entity should craft information security strategy in a manner that expects that shareholders will be watching every decision. Moving toward eliminating this agency problem, in the context of corporate information security, will improve accountability to shareholders for corporate losses resulting from information vulnerabilities. The improved disclosures described in Part III(A) will allow for even shareholders not knowledgeable in information security to track entities' progress (or lack thereof) in information control. Perhaps even more importantly, the additional proposed disclosures will eliminate an existing information disparity between the shareholders of an entity and third parties more knowledgeable about information security, i.e. the small group of hackers and information security professionals who scour the pages of information security industry publications for identities of vulnerable entities. Currently, these third parties know more about the information security practices of entities than most of the entities' shareholders. Through additional disclosures, shareholders will receive information that enables them to decide whether to sell their shares or communicate concerns to management regarding the entity's information security strategy.

b. Holding Vulnerable Entities Accountable in the Market and Diminishing Share Price

Additional information security disclosures will also assist marketmakers in exerting control over vulnerable entities. Marketmakers, provided they know about the information breaches, are in a position to hold entities accountable for inferior information security practices by punishing them with lowered stock price. Incorporating information security disclosures into a document that marketmakers are sure to read, such as a 10K, will ensure that marketmakers know of breaches as well. Consequently, they will be poised to react to the diminished intangible asset value of entities that have suffered repeated security compromise.

In at least two recent cases of severe information security breaches, tracking the share price of the entities raises doubts whether the diminution of intangible asset value that resulted from the security breaches was properly incorporated by the market. These two case studies of recent information

243. For discussions of the corporate decision making and problems related to proxy solicitation, see Mark J. Roe, *Delaware's Competition*, 117 HARV. L. REV. 588 (2003); Lucian Arye Bebchuk, *The Case for Shareholder Access to the Ballot*, 59 BUS. LAW. 43 (2003).

vulnerabilities are (1) the theft of the AOL customer list by a corporate insider and its sale to a spammer,[244] and (2) the penetration of Acxiom, Inc.'s database of personally identifiable consumer information by a hacker.[245] In both of these cases, the severity of the breach of information and the nature of the information breached is estimated to have resulted in millions of dollars in long-run losses for both entities. In light of these losses and in accordance with the efficient market hypothesis,[246] one would have expected that the stock price would decline to reflect the diminished commercial value of a critical corporate asset, but even several days after the market knew of the compromise, the stock price did not decline in either case.

i. AOL Customer List Sale to a Spammer

On June 23, 2004, a former AOL employee was charged with stealing the provider's entire subscriber list of 37 million consumers and over 90 million screen names, credit card information, telephone numbers, and zip codes and selling it to a spammer who leveraged and resold the information.[247] AOL had not previously acknowledged the data breach and knowledge of the breach was not widely possessed until the charges were brought. The AOL customer list was a critical intangible corporate asset of AOL whose value was contingent on its secrecy.[248] Therefore, it would be logical for the market price of shares of AOL's corporate parent, Time-Warner, Inc. to reflect a dip in value because of the incident and the corresponding diminution of a critical business asset's value. However, the share price on June 23 closed up and continued to increase for several days. In other words, it appears that the market price did not reflect an immediate change in share price as a consequence of a significant asset value diminution, as seen in Figure A below. It is possible that the share price corrected for this diminution later in the month, but it is also possible that the

244. Information regarding this theft was not publicly known until the arrest of the alleged perpetrator on June 23, 2004. *See* Sullivan, *AOL Customer List Stolen, Sold to Spammer*, *supra* note 117; *see also* United States Attorney, Southern District of New York, Press Release, U.S. Announces Arrests in Case Involving Scheme to Steal AOL Customer List and Sell It to Spammers, June 23, 2004, *available at* http://www.usdoj.gov/usao/nys/Press%20Releases/JUNE04/AOL%20Complaint%20PR.pdf.

245. *Id.*

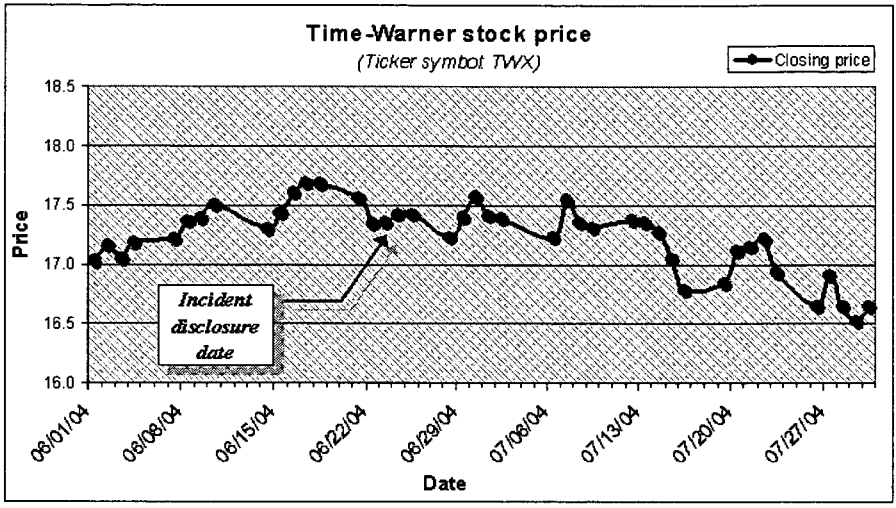
246. *See infra* note 255.

247. The software engineer who stole the data did not have immediate access to it himself; he was able to obtain the information through impersonating another employee. Although the initial sale price of the list is unknown, the spammer paid $100,000 for a second sale of updated information with 18 million additional screen names. The list was then resold to a second spammer for $32,000 and leveraged by the first spammer in his internet gambling business and sent mass marketing emails regarding herbal penile enlargement pills to AOL members. United States Attorney, Southern District of New York, Press Release, *supra* note 244.

248. Customer lists are considered a corporate asset and sometimes protectable under state level trade secret law, which varies from state to state in its scope. *See, e.g.*, Robert G. Bagnall, *Privacy*, SJ095 ALI-ABA 209 (American Law Institute—American Bar Association Continuing Legal Education, 2004) ("Although the value of a customer list may be difficult to estimate, it is clear that it may be a substantial asset.").

information simply never caught the attention of marketmakers and was not accurately filtered into share price.

Figure A. Closing Stock Price of Time-Warner Inc. – June 1, 2004 to August 1, 2004



ii. Hacker Penetrations of Acxiom's Consumer Information Databases[249]

Acxiom Corp. is a data aggregation company that sells aggregated consumer information to customers such as credit reporting agencies, banks, and the Department of Homeland Security.[250] On August 8, 2003, after the market closed for the day, Acxiom Corp. issued a press release that a significant breach of its databases had occurred. Social security numbers, credit card numbers, and telephone numbers belonging to several hundred thousand consumers were compromised in this breach.[251]

---

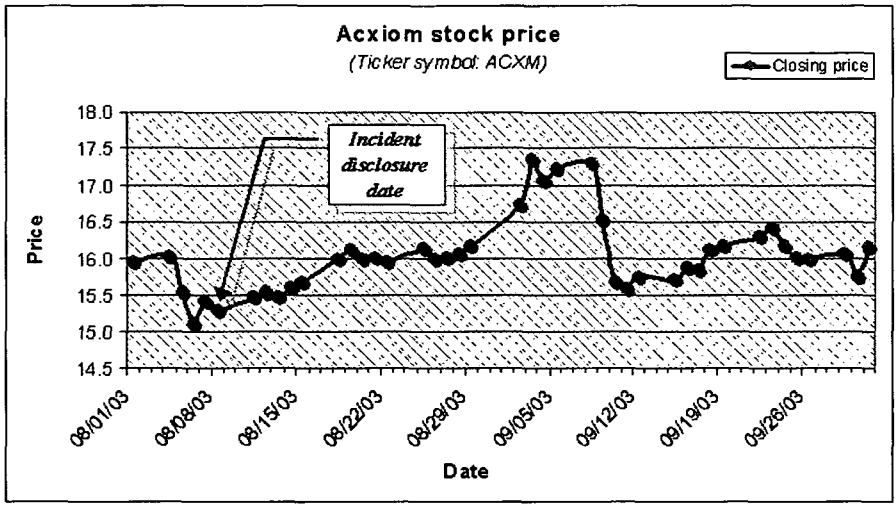
249. *See* Caryn Rousseau, *Hacker Accesses Customer Information from Database Manager Acxiom*, SECURITYFOCUS, Aug. 7, 2003, http://www.securityfocus.com/news/6665; Jay Lyman, *Acxiom Database Hack Highlights Risk*, TECHNEWSWORLD, Aug. 11, 2003, http://www.technewsworld.com/story/31306.html; Robert O'Harrow Jr., *Advertiser Charged in Massive Database Theft*, SECURITYFOCUS, July 22, 2004, http://www.securityfocus.com/news/9189; Associated Press, *Prominent Database Company Hacked Again, Florida Man Arrested for Huge Theft of Personal Data*, MSNBC, July 21, 2004, http://www.msnbc.msn.com/id/5481403; http://www.usatoday.com/tech/news/computersecurity/2004-07-22-Acxiom-hack-charges_x.htm; John Leyden, *Spammer Charged in Huge Acxiom Personal Data Theft*, THE REGISTER, July 22, 2004, *available at* http://www.theregister.co.uk/2004/07/22/acxiom_hack_charges; Laura Rohde, *Florida Hacker Indicted in Big Online Theft Case*, COMPUTER WORLD, July 22, 2004, http://computerworld.com/securitytopics/security/story/0,10801,94673,00.html.

250. The Department of Homeland Security is one of Acxiom's customers. *See* Jill D. Rhodes, *CAPPS II: Red Light, Green Light, or 'Mother, May I?'*, *available at* http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=107.

251. U.S. attorneys estimate the attack cost Acxiom $7 million, primarily from business lost or

The intangible assets compromised in this breach were Acxiom's prime assets. Consequently one would expect that the value of Acxiom's shares would be significantly diminished because of the diminution in value of the entity's prime assets. However, Acxiom's share price did not decrease in the days immediately after news of the data penetration became widely known to the market. In fact, Acxiom's closing share price increased steadily for several days after August 8, 2003, as shown in Figure B.

Figure B. Closing Stock Price of Acxiom Corp. – August 1, 2003 to October 1, 2003



Ultimately, two explanations are possible for the share price appearing not to demonstrate a downward shift. Either the vulnerable data had no market value and the stock price is correct without adjustment, or alternatively the vulnerable data had market value and the market failed to adjust. Customer lists and data assets initially have high costs of information acquisition but subsequent copies of the information cost almost nothing to "produce."[252] We know the "street" value of millions of AOL customers' information on the information black market[253] was over $100,000 and we can presume the value in the legitimate information marketplace is significantly higher, most likely

delayed. *See Alleged Acxiom Hacker Indicted*, http://www.4law.co.il/arkan1.htm.

252. For a discussion of increasing marginal returns, see BRIAN W. ARTHUR, INCREASING RETURNS AND PATH DEPENDENCE IN THE ECONOMY (1994).

253. Information black markets are increasing in size and scope. For example, outside of stolen client lists, one can purchase credit card numbers, zero day exploits and malware of various kinds. *See* Matt Richtel, *Rampant Trade of Stolen Credit-Card Numbers Shows Lack of Security*, N.Y. TIMES, May 12, 2002.

over $2,000,000.[254] However, in both the AOL and Acxiom breaches, the stock market appears to have failed to acknowledge this diminished intangible asset value, and neither entity's stock price appears to have been detrimentally impacted in the short-term because of these data vulnerabilities. Assuming the compromised data had monetary value, the market may therefore reflect an inefficiency based on the failure to adjust downward to reflect the lower value of a key asset of each entity. Thus, the market may not be compensating for weak information disclosure by incorporating the known security breach information from available sources into stock price.[255]

The explanation may be very simple: vulnerability information may simply not be catching the attention of marketmakers or perhaps these financial professionals, who are usually not information security professionals, may not yet understand the long-term financial implications of corporate information vulnerability. The field of information security is a relatively esoteric and new field, which did not gain prominence until the information technology revolution of the late 1990's. It is unreasonable to expect that marketmakers have the time or knowledge to scour the pages of SecurityFocus[256] on a daily basis to incorporate information about security breaches into their calculations of appropriate market price of entity's shares. Marketmakers need information in a usable format to which they are accustomed. The additional information security disclosures to annual filings proposed in this Part III provide one such usable format.

---

254. For example, the value of the 250,000 customer list of a bankrupt online retailer was deemed to be worth at least $50,000. *See* Gavin McCormick, *Settlement Reached in Toysmart List Case*, CLICKZNEWS, Jan. 12, 2001, http://www.clickz.com/news/article.php/559231.

255. Doubt is yet again cast on the efficient market hypothesis. Fama asserted a market is efficient if there are large numbers of rational profit-maximizers competing to predict future market values of securities with information being almost freely available to all participants. In an efficient market, actual prices of individual securities already accurately reflect the effects of information based both on events that have already occurred and which will take place in the future. In other words, an efficient market's actual price of a security will be a good estimate of its intrinsic value. *See, e.g.*, Eugene Fama, *Efficient Capital Markets: II*, 46 J. FIN. 1575 (1991). *But see* Andrew K. Rose & Olivier Jeanne, *Noise Trading and Exchange Rate Regimes* (Reserve Bank of New Zealand Discussion Paper No. G99/2, 1999), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=348200. In fact, what we know from complexity theory is that the most efficient systems are not those where information is perfectly incorporated but rather systems with some noise. *See, e.g.*, Wouter-Jan Rappel & Alain Karma, *Noise-Induced Coherence in Neural Networks*, 77 PHYSICAL REV. LETTERS 3256 (1996), *available at* http://physics.ucsd.edu/~rappel/pub/coherence.pdf. The explanation adopted here is that the nature of information security information is currently too complex for most investors and analysts to be able to understand and incorporate into their investment decisions. A market failure to absorb complicated information security information into stock price might be paralleled with the inability of the market to absorb information about the complex legal issues involving environmental damage, which resulted in the SEC's addition of line item disclosures to Regulation S-K previously, and the questionable nature of Enron's transactions. Even as copious information about the dubious nature of Enron's activities was available to marketmakers, Enron's share price continued to climb. *See, e.g.*, Lawrence Evans, Enron and Chaos, http://www.ecotao.com/holism/add/enron/Enron_chaos.html. Markets do not exist in equilibrium; they strive for equilibrium but frequently fail.

256. For example, Security Focus recently broke the story of the leakage of 500,000 credit card numbers by a vulnerability in the PetCo, Inc. website. *See* Poulsen, *supra* note 171.

3. System

With regard to the final element of system, three systemic benefits will result from this exercise of additional control arising out of new communication. First, market stability will be bolstered in a manner consistent with prior practice, minimizing the disruptions to the existing system. The Securities and Exchange Commission would help create a system to address the information security crisis by using existing regulatory structures and following its own model from the previous regulatory policy challenge of improving corporate environmental practices. Secondly, publicly traded entities themselves will benefit through encouragement to put in place more systematic processes of information control and self-assessment. Focusing on improving information security practices will assist entities in protecting proprietary information and creating value in the long run. Finally, a last systemic benefit may happen through the employees of entities. Entities will begin to train their employees in rudimentary information security and the importance of data control. Ideally, these behaviors, once implemented throughout organizations by employees, will be accompanied with the positive externality of employees transferring good information security behaviors into their personal behaviors as well. Consequently, the portion of information vulnerability in our economy resulting from suboptimal consumer security behaviors may be reduced.

a. Bolstering Market Stability: Using Existing Structures of Securities Law

The idea of crafting more data privacy and security legislation is an idea proposed frequently as the best approach to improve the information security crisis faced by our society.[257] However, prior to investing additional Congressional resources into drafting new statutes and generating entirely new data control regimes that will potentially disrupt existing corporate and legal structures, we should first exhaust the capabilities of existing legal regimes in

257. *See* Emily Frye, *The Tragedy of the Cybercommons: Overcoming Fundamental Vulnerabilities to Critical Infrastructure in a Networked World*, 58 BUS. LAW. 349 (2002) (advocating Congressional intervention into commercial data security through new legislation requiring corporate disclosure of actual cyberintrusions and measurable damages). For a general discussion of legal implications of commercial data security, see Wendy Meyer, *Insurance Coverage for Potential Liability Arising from Internet Privacy Issues*, 28 J. CORP. L. 335 (2003) (arguing that in light of new internet liabilities, insurers must create new policies to create such liabilities, particularly for gathering of private information through the internet); Thomas J. Smendinghoff, *The Developing U.S. Legal Standard for Cybersecurity*, 4 SEDONA CONF. J. 109 (2003) (arguing corporate security law is emerging and requires constant vigilance by business entities); Tal Z. Zarsky, *"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 4 (2002-03) (arguing that the market in personal information demonstrates market failure and that a public opinion campaign should be mounted to find a solution to problems associated with data mining tools); Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11 (2002) (arguing for adoption of traditional negligence law principles in the context of information security); Rustad & Eisenschmidt, *supra* note 209 (arguing proposed Article 2B of the Uniform Commercial Code is a legal framework ideally suited for resolving legal issues which arise in connection with internet security products).

alleviating the information security crisis. The securities law approaches proposed in this article hold promise as methods of improving corporate information security practices without the upheaval and protracted process required by crafting new legislation. The speed of information security evolution requires a more nimble approach that a regulatory body such as the SEC with faster response times than Congress is better suited to provide.

Similarly, the mark of a good corporate legal regime is one which effectuates socially necessary changes in corporate behavior without overburdening entities through excessive new legislation, what Professor Ribstein might term "humble" regulation.[258] Put another way, a well-crafted legal intervention into corporate behavior will dovetail compliance with new legal requirements with an entity's existing processes of enterprise risk management planning and compliance processes. Consequently, a new legal regime should attempt to use compliance mechanisms that will be incorporated as seamlessly as possible into the life of a business entity while simultaneously furthering the social purposes that necessitate the legal intervention. In this manner, society moves toward an economic system where consumer protection is harmonized with a process which assists entities to pursue long-term economic gains for shareholders.

Perhaps most convincingly, precedent for improving corporate information security using securities law already exists: our society faced a similar problem almost a decade ago in the context of environmental liabilities. Congress has legislatively highlighted the social importance of information security in a manner similar to the way Congress highlighted the social importance of environmental protection in the 1980's with the passage of CERCLA[259] and other environmental legislation.[260] In the 1980's, the SEC worked to implement the Congressional directive of better corporate environmental practices by correcting a similar disclosure and possible market adjustment failure. Accordingly, the SEC required increased corporate disclosure of potential environmental liability in the MD&A section of securities filings.[261]

---

258. Larry E. Ribstein, *Sarbox: The Road to Nirvana*, 2004 MICH. ST. L. REV. 279.

259. The Comprehensive Environmental, Response, Compensation and Liability Act, 42 U.S.C. § 9601, known as "CERCLA" or the "Superfund" law, is the principal federal law governing the cleanup of pollutants and the remediation of polluted sites.

260. *See* United States v. Reilly Tar & Chem. Corp., 546 F. Supp. 1100, 1112 (D. Minn. 1982) (summarizing CERCLA's congressional legislative history); *see also Fifth Annual Symposium on the Topic of "Disclosures of Environmental Liability in SEC Filings, Financial Statements, and Debt Instruments," Opening Remarks of the Panelists*, 5 VILL. ENVTL. L.J. 293 (1994).

261. The addition of a line-item environmental disclosure requirement by the SEC was necessitated in part due to doctrinal confusion in standards of "materiality" for MD&A disclosure. This doctrinal uncertainty has remained unresolved and, hence, we face a similar problem in a different policy context now. However, the information security crisis cannot wait for this doctrinal resolution of the materiality standard.

b. Facilitating Corporate Value Creation: Building Effective Enterprise Risk Management Processes

Because the threat of regulation and liability appears to be the strongest motivating factor for corporate security improvements,[262] a line item disclosure requirement will motivate corporate entities to focus corporate resources on information security. However, as mentioned previously, investments in information security by entities have clear long-run benefits for the entity itself. Better security results in public relations benefits,[263] including maintaining customer satisfaction and preventing customer churn, preservation of differentiating intellectual property, and competitive advantage. These benefits position the entity to demonstrate due care with trade secrets to a court,[264] avoiding breach of privacy policy promises to users and avoiding liability associated with regulatory agency prosecution. Similarly, instituting strong information control assists entities in knowledge management[265] to be able to harness information resources more easily for corporate ends. As a consequence of prudent information security risk management planning, information security will no longer be viewed as exclusively the province of information technology departments of corporations but rather the joint responsibility of all employees of the entity since information security is an enterprise-wide undertaking. Raising institutional awareness through securities law will bring new groups of corporate management into the information security strategy process. Entities will begin to recognize the information transformation they have undergone in the last decade, as well as the increased importance of information systems in their operations. Information regarding information breaches will be shared more widely within entities and their importance more carefully assessed.

Secondly, the mere act of completing securities disclosure forms frequently acts as a catalyst for corporate officers to sit down with their in-house and outside counsel to collect and assess information they will be providing to the market. Securities filings with particular disclosure requirements can be viewed

---

262. Ware, *supra* note 102.

263. Breaches of data security frequently bring with them bad publicity. For example, Oracle recently suffered a public relations debacle when its allegedly "unbreakable" database technology was penetrated. Avoiding such bad publicity preserves the goodwill of an entity and having processes in place to manage the incident and its consequences reflects good management. *See* Thomas C Greene, *How to Hack Unbreakable Oracle Servers*, THE REGISTER, Feb. 7, 2002, *available at* http://www.theregister.co.uk/2002/02/07/how_to_hack_unbreakable_oracle/.

264. If an entity has experienced significant data compromise and does not take action to improve its security, demonstrating to a court in the case of trade secret litigation that corporate proprietary information has been kept secret with due care becomes more difficult. As receiving trade secret protection for a particular intangible asset is contingent on this demonstration of care and secrecy, entities will benefit in the long run from crafting stronger information security management practices and building processes to review their efficacy on an annual basis.

265. For a discussion of the definition of knowledge management, see CIO, The ABCs of KM, http://www.cio.com/research/knowledge/edit/kmabcs.html.

as a reminder to management of key sources of liability for entities. Particular line item disclosures on information security will ensure that these decisionmakers spend time at least once a year reviewing their entities' information security policies and losses.

c. Consumer Protection: Consumer Information Security Behavior Learning Through Employees

Finally, because corporate information security is an entity-wide enterprise, a critical mass of employees in each entity will progressively become trained and sensitized to protecting the corporate proprietary information. Consequently, a positive externality may result: some of the good corporate information security practices these employees learn may be applicable, and thus, transferable outside the workplace to their handling of their own sensitive personal information. Correspondingly, a portion of the consumer information vulnerability problem may begin to decrease. For example, the entities in the sample in Part III employed 3,458,544 people. If even half of these individuals become more informed consumers, improve their personal practices with regard to information security, or teach family and friends about information security because of training they received for the benefit of their employers, significant progress toward alleviating the information security crisis is likely.

IV. CONCLUSION

In this article I have argued that our society exists in a state of information security crisis. Congress's attempts to date to address this crisis adopt the largely discredited cryptography and security paradigm of "security through obscurity." These attempts do not focus on analyzing and addressing information security problems in the economy as a whole, and therefore, are not destined to stem the information security crisis we currently face. A better regulatory approach is one that adopts concepts articulated by Kerckhoff's Law—that of "security through process." It also adopts lessons from complexity and cybernetics theory about information transfer in a scale-free system, particularly regarding the importance of constructing feedback loops and contemplating network properties of risk and behavioral transitivity. Similarly, an empirical examination of information security disclosure practices of 120 publicly traded entities demonstrated that correcting the regulatory approach is necessary because the conduct of a vast majority of these entities also reflects a paradigm of "security through obscurity." Therefore, security learning is unlikely to emerge in the marketplace without legal intervention and assistance.

As such, the SEC should now follow its own example from the environmental disclosure context and replicate it in the information security context: the SEC should again remedy disclosure and possible market

adjustment failure through creating additional line item disclosure requirements that implement the Congressional directive of better corporate information security practices. As such, because the harms of information crime are shared by business, government, and consumers, a paradigm of "security through obscurity" does not acknowledge these shared consequences of security failures. Meanwhile, a process-based approach addresses these issues of shared control in a superior manner. Requiring line item information security disclosures will help increase awareness of the information vulnerability crisis our society faces and scaffold learning of better information security practices for both corporations and consumers. Security is ultimately not only about one entity's or one consumer's proprietary information; it is also about protecting the good of the social information ecology as a whole and stemming information harms to better enable commerce and innovation.