Considering Data Breaches: Public Information, Corporate Responsibility, and Market Valuations

Kristopher Dane

A capstone project presented in partial fulfillment of the requirements of the degree of
Master of Arts in Policy Studies
Interdisciplinary Arts and Sciences
University of Washington
June 2012

The electronic approval accompanying this capstone manuscript affirms that the work has incorporated all necessary revisions and is satisfactory.

First Reader:

signed electronically on June 1, 2012

Dr. Dan Jacoby
University of Washington

Second Reader:

signed electronically on May 31, 2012

Dr. Cinnamon Hillyard
University of Washington

CONTENTS

ABSTRACT

This study examines the relationship between data loss incidents and stock price impact by exploring the question of whether the stock price impact of a corporate data breach differs depending on the nature of the breach. To date studies of this kind have been limited and have used ad hoc methods. Here we explore whether differences in the type of data breach have an impact upon stock prices. In general studies of stock impacts are helpful because they may suggest the real costs of data breaches if the market efficiently processes that information. It is also useful to know whether stock price losses can serve as an appropriate self-regulatory device providing incentives to prevent data breaches. Although limited, the results in this study suggest that the stock market may not fully anticipate losses from data breaches.

CHAPTER 1 – PURPOSE OF THE STUDY

PROBLEM STATEMENT

Cyber criminals pose a growing threat to corporate and personal information. Although governments have focused on the problem of information security for decades, rising dependence on digital data both for personal and corporate use has led to an increase in opportunities for cyber criminals to benefit from illegal access to that data. High profile data loss incidents at Honda, NASDAQ, Sony, and government contractors, RSA Security, Lockheed Martin, as well as warnings from several national governments about data security have begun to heighten concern within corporations. Data security is no longer just an additional job responsibility for the information technology department, rather, it has grown into a unique risk management role within the company (Dunham, 2012). Several corporations have created a new executive level position called the Chief Information Security Officer and have started to adopt information assurance standards from NIST and ISO. Academics are increasingly looking at the costs of e-commerce programs to corporations such as the impact of new web-based initiatives and data loss incidents on stock price. Recognizing that the risk posed by data-loss is multifaceted, this study digs deeper into the relationship between data loss incidents and stock price impact by exploring the question of whether the stock price impact of a corporate data breach differs depending on the nature of the breach.

In looking at the stock price impact, this research contributes to the debate about the appropriate role for government to play in the information security space. This on-going debate spans from broad concerns about the national defense of “digital borders” to the protection of personal information and is thereby shaping legislation that may control the future of the information security field. A key pillar in this debate is the tension between the role of government to ensure the safety of its citizens versus the ability of the market to achieve efficient solutions on its own (Brennan, 2012).

On one side, the federal government officials claim that private ownership and control over the

internet severely limits their ability to gather intelligence and respond to attacks from opposing nations or international cyber criminals (Sullivan, 2012) . These attacks are responsible for harm to national security, the privacy of citizens, and to the intellectual property of corporations. The only way to respond, say some in the Department of Defense, to these attacks is to collect better intelligence and build up our cyber military. This approach requires that government secure more information about attacks on the network at large which includes monitoring private network data (Schrier, 2011). The government's role should at least be to set minimum standards for data security similar to the safety standard set in the aviation industry says John Brennan, President Obama's counterterrorism and homeland security advisor, "We have these standards when it applies to the aviation industry. We have it on so many different areas, I would think that the American would like some assurance that the water that they drink, that the electricity that they rely on is going to be protected. And we well know that they cyber threats that are out there are just growing every day" (Brennan, 2012).

On the other side, increasing government regulation is resisted by corporate interests that claim that regulations increase cost without contributing to security (Brennan, 2012). In an open letter regarding the proposed Cyber Intelligence Sharing and Protection Act (CISPA), the Completive Enterprise Institute wrote that the regulation, "risks unduly expanding federal power, undermining freedom of contract, and harming U.S. competitiveness in the technology sector" (Radia, 2012) . Government response has typically been that corporate recognition of these risks and increasing action to limit data breaches is a result of regulations mandating data breach disclosure. It is government regulations, not efficiency and consumer choice, that has driven corporations toward more responsible data protection.

This study connects and informs the disparate information security debates taking place in some corners of the legislature, top secret government installations, corporate board rooms, and in various academic disciplines. Further, the study contributes to overarching premises of market self-regulation by studying the near-term stock price impact on corporations of data

breach announcements. This study speaks to the extent to which the market already addresses the security of personal data.

SCOPE OF THIS STUDY

Study seeks to define the broad implications of the policy problem while also answering a narrowly defined set of questions about the indications of market regulation. This study examines data breach announcements from the years 2000 to 2012. It is limited to considering corporations traded on the New York stock exchange and the NASDAQ stock exchange.

This study includes many terms that are technical in nature and are either not present or are misunderstood in the public debate. As a result, several key terms are defined in Appendix A.

CHAPTER 2 – LITERATURE REVIEW

BACKGROUND

Cybercrime is an increasingly important source of revenue for transnational criminal organizations attracted by its low risk and high rewards. Whereas, government has a unique and critical role to play in combating transnational crime in general, the mobile nature of cybercrime poses a unique challenge to corporations.

The President's *International Strategy for Cyberspace* (Obama, 2011) proposes a $3.4 billion budget to boost the cyber defenses of the Department of Defense signaling cybercrime's high priority within his administration (Wolf, 2012). However, prosecutions of cyber-crime are sparse (Caldwell, 2011). Federal law enforcement authorities have found it difficult to cooperate with their international counterparts on investigation, prosecution, and extradition of cybercrime. Without such cooperation criminal hackers take advantage use regulatory arbitrage to maximize profits. Aligning legal standards may help alleviate some of the problems and increase the chance for prosecution but establishing international cooperation over cybercrimes at the United Nations has proved challenging (Computer Weekly, 2010). There are signs that some of these barriers to cooperation are being removed as demonstrated by the recent arrests of several high profile hackers however the result of those arrests and the possibility for extradition are far from clear (Dunham, 2012). It may take years before we know if these are genuine steps toward international cooperation on fighting cyber-crime or if the arrests are the results of short term political maneuvering. In the meantime, both government and corporations are left to defend their own networks against an increasing flow of attacks.

GOVERNMENT ACTION

For years, governments have led the way in the development of information security management systems (Cerdes, 2009). Despite their leading role cyber attacks on government have not abated. In March of 2012 the Office of Management and Budget released a report that stated that "the number of computer security incidents reported to the U.S. Computer

Emergency Readiness Team (US-CERT) that impacted government agencies rose 5%, to 43,889" and, according to the Government Accountability Office (GAO), the number of federal security incidents have increased by 650% over the past five years (Moyle & Kelley, 2012). The same GAO report cited weakness in the implementation of security controls, indicating that there is room for improvement even among the leaders in this field. The steps to improving the performance in the government agencies is similar to the steps to improve information security outside the government: get buy-in from the leaders at the top (not just the security leaders), and build user awareness from the bottom up including discussing the threats of new technologies such as virtualization and cloud computing (Moyle & Kelley, 2012). In fact governments have contributed to the information security of the private sector by setting the standard for information security management programs. The Computer Security Division at the National Institute of Standards and Technology (NIST) has published a series of documents defining the standard to which federal agencies are held accountable. The series, known as the "800 Series" covers the range of security controls from "800-12: The NIST Handbook: An Introduction to Computer Security" to "800-53: Recommended Security Controls for Federal Information Systems and Organizations" (Computer Security Division). These standards are publically available for private corporations to access and incorporate into their policies.

CORPORATE ACTION

Responsibility for information security has typically fallen within the domain of information technology personnel in corporations. This approach reflects the way that security has been treated within the software industry as a whole. Security has been thought of as a "bolt-on" fix rather than "baked-in" during the development of software. Because the internet was not designed with security in mind, forensics are difficult and the prosecution of cases becomes more problematic (Endicott-Popovsky, 2011). Given corporate vulnerability to costly breaches, information security has moved "up the chain" with the creation at an executive level of the Chief Information Security Officer. The creation of this position reflects the reality that, in the words of a senior executive, "we are all IT companies" and there are significant risks associated with that reality (Pierson, 2011). The risks stem both from the reliance on the data as well as

the innovative nature of the threat to that data (Symantec threat report). Data security can no longer consist of just locking the door to the server room, buying the latest anti-virus software, or the newest firewall. Cyber criminals are increasingly adept at exploiting any vulnerability an organization has in its information security management system.

Cyber-criminals target information through a variety of means that range from taking advantage of software vulnerabilities to social engineering. Attacks on applications ranges from injection attacks where user input is not checked for malicious code to taking advantage of security misconfiguration, to more sophisticated methods. These advanced methods include cross-site-request forgery (CSRF) where, “the attacker force[s] the victim’s browser to generate requests that the vulnerable application thinks are legitimate requests from the victim” (Open Web Application Security Project). Not all attacks are solely focused on software vulnerabilities; social engineering is increasingly being used as a method of attacking corporate networks including leading security firms (Covielo). Social engineering takes place when, “an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems” (United States Computer Emergency Readiness Team). The outcome of each of these attacks is the same, however, private information about corporations or personal information about consumers is taken from databases that belong to corporations into the hands of malicious actors.

The threat to information is real and diverse and corporations are responding. This response includes creation of the Chief Information Security Officer (CISO) position and adopting the NIST 800 series or its international equivalent, International Standards Organization 27001. Both the NIST 800 series and the ISO 27001 standard outline corporate approaches to information security management systems. This process includes outlining business objectives, assessing risks, enacting controls, and constantly monitoring implementation and review. In addition, a new interdisciplinary community is taking hold around issues information security that includes non-governmental organizations such as the Information Systems Security Association (ISSA), public-private partnerships such as Infragard (Infragard), and the creation of new professional

security certifications such as the Certified Information Systems Security Professional certification (ISC2).

These organizations, with the help of government funding, have spurred the creation of academic programs that are separated from the computer sciences training and have a singular focus on information security. These security programs provide training for security professionals but they are also reach out to computer science programs in order to push them away from the "bolt-on" approaches toward the "baked-in" security that is necessary. Microsoft has led the move toward secure software development with the creation and public promotion of the Security Development Lifecycle (Lipner & Howard, 2005). Computer science programs such as the Computing and Software Systems program at the University of Washington, Bothell have also indicated an interest in incorporating security as a central focus of their software programming curriculum (Endicott-Popovsky, 2011). The threat landscape is changing rapidly, "The cyber-security skills needed three years ago compared to now '[are] a whole different ballgame'" (Marsan, 2012).

CONSIDERING THE ECONOMICS

Having established the background and a summary of the actions that have been taking place in information security problem space, it is important to take a step back and consider the role of public policy. Jonathan Gruber's text *Public Finance and Public Policy* (2011) outlines four questions that are relevant to the role of government in the economy:

1) When should government intervene in the economy?
2) How might the government intervene?
3) What is the effect of those interventions on economic outcomes?
4) Why do governments choose to intervene in the way they do?

Governments, Gruber says, intervene in the economy for two reasons: efficiency or equity. When markets are not achieving the efficient outcomes, this is called market failure, and

governments step in to correct the failure through a variety of means. Sometimes, however, market outcomes are not equitable and government steps in to redistribute wealth throughout the society. The government intervention can take many forms and ranges from setting tax policy to subsidizing particular sales or purchases to public provisioning where the government takes over the distribution of the good. These government interventions have diverse effects some of which are intended and some of which are unforeseen. The decision to intervene and the choice of intervention method are contested decisions that are the outcome of political bargaining between government agents and private actors and other stakeholders.

Of Gruber's questions listed above, the two that are most relevant to this study discussion are the first two concerning why governments intervene in the economy and what form that intervention should take. The common definition of efficiency is "gaining the most output for a given level of input or getting 'more bang for the buck'" (Birkland, 2005, p. 161). Public policy solutions then are judged on their ability to restore efficiency to the market. Policy makers strive to achieve Pareto efficiency which is when "no alternative allocation can make at least one person better off without making anyone worse off" (Smith & Larimer, 2009, p. 108). The problem is that Pareto efficiency only results when in truly competitive markets which are rare in reality. Markets suffer from market failure where Pareto efficiency is not achieved as a result of imperfect information, externalities, or because of the nature of the good.

INFORMATION

The existing literature discussing the issue of information in the market for information security comes from a variety of academic disciplines. Criminologists distinguish between the legal market for information and the illegal market for information. The legal market includes the collection, storage, and sale of non-personal information for their purposes of marketing. In this legal market, they find no market failure (Cerdes) since consumers benefit from the targeted advertising that is provided as a result of the non-personal data collected. One remaining issue in this discussion centers around the equity concerns of the possibility for differential pricing based on collection of data about the tastes of individual consumers. While there are concerns

over the privacy of consumers, economists find that this kind of differential pricing allows for pricing that more closely matches individual willingness to pay (Montagne, 2011 & Rubin & Lenerd, 2005). The market for illicit information, on the other hand, presents a series of challenges including imperfect information and externalities.

Economists William Roberds and Stacey Schreft (2009) take a narrow view of the market for legal information. Roberds and Schreft analyze the notion of "efficient confidentiality" (Swire, 2003) by considering the market for credit based purchases. They outline the benefits of the credit-based payment consumption? system by drawing on monetary theory. Roberds and Schreft describe the market for consumer information by describing a person's confidentiality as an economic good whose provision depends on two other goods:

- the amount of PII incorporated into that persons transactional identity
- the level of security for these data or the degree of data integrity (Roberds & Schreft, p. 26)

Consumers can be more accurately identified by increasing the volume of data that is included in the consumer's transactional identity. That is, as the payment processors know more about the consumer, the easier it is for them to reduce account fraud. At the same time, however, increasing the amount of PII collected about a consumer reduces their privacy and increases the impact if the data are misused. An efficient system is thus one in which the additional benefits of adding collecting PII are equal to its additional costs (Roberds & Schreft, p. 26)

As discussed above, the efficient allocation of a good through the economy relies on clear and accurate information. Roberds and Schreft argue that while consumers can be informed of the amount of PII incorporated into their transactional identity by monitoring their credit reports and the privacy statements provided by service providers, they cannot access information on security of these data. In fact, the cost to individual consumers of monitoring their transactional identity is quite high. Despite the fact that many thousands of transactions can happen on an

individual's account in a year, consumers only have access to one free credit report per year (Central Source LLC). Furthermore, that credit report does not include the important FICO credit score which oftentimes determines eligibility for access to credit. Consumers must pay to access that part of their transactional identity.

There is even less information available to the consumer on the security measures employed by corporations to protect consumer data. While corporations are required to outline all anticipated uses for consumer data in privacy statements, there is no such requirement for disclosing the security measures that protect customer data. In all but 2 states, mandatory data breach notification laws are in place that require consumer notification when their PII has been lost or stolen. The definitions of what constitutes PII, what constitutes a breach, and what the threshold is vary greatly from state to state but it is important to note that the company does not have to disclose the new security procedures in place to protect the data. Whereas laws such as Sarbanes-Oxley require particular auditing of financial records via third-party auditors and statements to the Securities and Exchange Commission, there is no similar standard for information security standards. Consumers and investors then cannot choose between corporations on the basis of data security standards.

The lack of information is not simply a lack of training on the part of the employee or a lack of oversight on the part of the corporation; it is a mixture of the two. The most commonly cited concern in this area is the market failure as a result of information asymmetry. The information asymmetry exists between firms and between firms and consumers (Kannan, Rees, & Sridhar). Firms collect information on attacks but do not share it with each other as it may show that they are a target or possibly damage their reputation. This lack of sharing harms other firms who are not able to respond or prepare for similar attacks. In addition, when firms do not release information about data breaches, the consumer is potentially damaged by identity theft. In addition, this lack of information places investors at a disadvantage when it comes to assessing the risks management position of a firm.

EXTERNALITIES

In addition to incomplete and imperfect information, another source of inefficiency in markets comes from externalities. An externality occurs "whenever the actions of one party make another party worse or better off, yet the first party neither bears the costs nor receives the benefits of doing so" (Gruber, 2011, p. 122). A negative externality occurs when one party does not take into account the full cost of his actions to others. Roberds and Schreft identify two sources of externalities in the market for information: attribution and cost recovery. Successful functioning of the credit market requires a large number of organizations to have access to the data and as a result data security becomes a "weakest link" or "flood control" good where the total amount of security is at the mercy of the actor that invests the smallest amount into security (Roberds & Schreft, p. 26). Due to the large number of actors involved, it is almost impossible to attribute fraudulent activity to the lax security of a particular corporation. Businesses commonly try to transfer the risk to contractors. The problem, says Philip Alexander the Information Security Officer at Wells Fargo bank, is that "…companies that have third-party firms maintain customer data for them are still liable if the data is breached. I call that outsourcing the work while 'in-sourcing' the liability! Third party firms are only responsible for notifying the companies they service that they have suffered, or may have suffered, a data breach. The data owner is still liable to disclose the breach to its customers" (Alexander, 2007). So the contracting companies do not have an incentive to provide security since they will not bear the cost of the data breach. Even if it was possible to hold the contractor responsible, recovering the losses through the courts is itself costly (Roberds & Schreft, p. 27). The losses to the economy are quite large.

The FTC estimated that losses due to identity fraud in 2006 equaled $49.3 billion in the United States. Once time and additional expenses are factored in, that cost is estimated at $61 billion (Schreft, 2007). If we consider the other expenses caused by lax data security such as loss of intellectual property, the number increases by another $53 billion (ASIS Foundation, 2002). In

addition to the loss of personal information and the loss of intellectual property, lax data security poses risks to national security.

NATURE OF THE GOOD

The growth of the internet and the importance of security goes beyond the discussion of private data, however, the problem "has become the concern of everyone who uses information and that seem[s] to include every one of us. With this in mind, we are obliged to discuss security beyond the network so that everyone is who is unknowingly or knowingly involved is brought into the dialog of securing the information systems that are increasingly controlling our lives." (Kizza, 2009). The reality of the collective responsibility for security on the internet is becoming apparent with the growing discussion of the risks to critical infrastructure in the United States. These attacks on dams, power utilizes, and water treatment facilities via the internet are commanding more and more attention from the public and from the government. In fact, the United States has itself taken advantage of the vulnerability of critical infrastructure to attack as shown through the development and use of the Stuxnet virus to delay Iranian nuclear progress. The United States itself has been experiencing attacks on critical infrastructure facilities. These attacks take advantage both of the fact that critical infrastructure is increasingly connected to the internet but also taking advantage of the fact that security is often not a central goal of the utility operators. With 90% of the internet being owned by private parties, the government has no authority to secure those networks.

It is the interdependence of internet users that seems to suggest that secure use of the internet is a public good. A public good is one that is non-rival in consumption (one person's use does not diminish another person's use) and is non-excludable (one person cannot deny another person the opportunity to consume the good) (Gruber, p. 182).

ACADEMIC RESEARCH

In light of these potential challenges to the efficient functioning of the market, scholars from a variety of disciplines have begun to explore the impact of data on companies.

Subramani and Walden looked at the impact of e-commerce announcements on stock price (Subramani & Walden). Others have looked at the specific impact of data breach announcements on the stock price of corporations and found a statistically significant (Goel & Shawky). In a unique analysis drawing on operations management, decision tree analysis has been used to build an ex-ante model of stock price impact (Andoh-Baidoo & Osei-Bryson). Including firm size along with the data breach characteristics explains some of the cross sectional variation in stock price (Cavusoglu, Mishra, & Raghunathan). Smith and Smith look at the effect of cybercrime on stock price performance (Smith, Smith, & Smith).

We know that the prevalence of cyber-crimes is based on an economic calculation of stocks of hacking skills relative to economic opportunity and, critically, the attacker's selection of target is based on not only symbolic significance but also weakness in defense mechanisms (Kshetri, 2005). Ethnographic studies have shown that hackers are rational with hackers who are more rational engaged in preparation, reconnaissance, and attacks that were more successful than their more impulsive counterparts (Bachmann, 2010). Cyber criminals engage in cyber-crime because they know of the diminished chances of being caught (Jaishankar, 2011, p. 59). Government could change the incentives in this calculation but it is unlikely to do so soon so corporations must continue to develop mitigation strategies for the threats they face (Wong, 2011).

POLICY OPTIONS

In the discussion above about the larger market for information, we discussed several aspects that may justify public policy intervention: information problem, externalities, the nature of the good. Further academic research has been looking into the possibility that the market is self-regulating. Recent legislative focus in the information security area, however, has been focused on addressing the national security concerns rather than addressing the challenges to privacy and data breaches (Jackson, 2012). Here we outline one way in which public policy might be used to address the problems posed by data breaches.

Innovative research at the University of Maryland has shown that the attacks vary with the population and are most common when the traffic on the network is highest (Engineering Information Institute, 2011). Professors Cukier and Maimon analyzed the attacks on the campus and concluded that a "computer network's social composition will determine where [the] attacks come from." Cukier and Maimon found that the nature of threat changed depending on the time of day. This change in attacks was caused by the increased number of unsecured devices on the network during business hours as well as by, what Cukier and Maimon call, the "human aspect". Users they say, "…expose the network to attacks. Simply by browsing sites on the Web, Internet users make their computers' IP addresses and ports visible to possible attackers. So, the user's behavior does reflect on the entire organization's security" (2011). This process of threat evolution is taking place on the internet at large as an increasing number of mobile devices connect to browse and conduct financial transactions over the internet. Cukier and Maimon's research point to two potential solutions (2011):

- Increased education and awareness of the risks associated with computer-assisted and computer-focused crimes among network users could prevent future attacks;
- Further defense strategies should rely on predictions regarding the sources of attacks, based on the network users' social backgrounds and online routines.

There is little academic work on the awareness question, though NIST makes security awareness and training part of its overall information security management system. In addition, NIST has published another document that talk about educating users. There is little more that government can do to directly inform individuals than the typical press releases and making this issue a matter of sustained attention in the legislature and executive agencies.

There is a bit more that can be accomplished to advance the second recommendation to improve predictions on the sources of attacks. Predictive warning are the most passive way in which public policy can improve the state of data security. Sharing attack information across public / private lines as well as between private corporations will contribute to security by

building an understanding of the nature of attacks, their origin, and would allow for much more rigorous analysis than what is available with the ad-hoc data presently in use.

Proposed national collection efforts contained in CISPA focus on collecting cyber-attack data for the purposes of protecting critical infrastructure but that same information could be used to protect the corporate networks that are holding the private information of individuals. Local efforts at collecting government and private network data such as PRISEM in Washington state have proved difficult due to privacy concerns but due to concerns over liability but these problems may be overcome by a national regulatory scheme that makes strides toward privacy and allows for sharing of critical attack data.

The Department of Homeland Security is working with the Defense Department on developing the Joint Cybersecurity Services Pilot program which is an evolution of the Defense Department's information sharing scheme called the Defense Industrial Base (DIB) (Wolf, 2012). The DIB involves sharing sensitive threat-related information between the government agencies and selected corporations. Ashton Carter the deputy secretary of defense stated that, "Increased dependence on Internet solutions have exposed sensitive but unclassified information stored on corporate systems to malicious probes, theft, and attacks. This expanded partnership between DoD and the defense industrial base will help reduce the risk of intrusions on our systems." (Office of the Assistant Secretary of Defense (Public Affairs), 2012). Programs such as the DIB are a first step toward sharing information security information but, for these programs to work liability concerns must be addressed, security concerns must be addressed, and the information must be available to as many people as possible so they can respond. Once set up, however, an information exchange would, "inform consumers of potential risks and encourage companies to ensure adequate protection, but also to provide information to businesses, organizations, and government on the true scope of the problem for proper risk assessment" (Picanso, 2006).

CATEGORIZATION OF DATA BREACHES

There are many ways in which a corporation can lose data. As a result, data breaches are classified differently across various analyses. Here we have adopted the most recent and thoroughly explained classification schema developed by security experts Matthew Curtin and Lee Ayers (2009). Curtin and Ayers split data breaches into three main categories: Physical, Logical, and Procedural breaches.

Physical breaches are those in which there is a loss of physical control over the data. Physical losses are characterized by the loss of documents, computers, and media such as compact discs, tapes, and other drives.

Logical breaches are those in which there has been a failure of the information security management system. That is where the controls in place were exploited by employees (insider threat) or outsiders (hack). These breaches occur due to a "loophole" in the security systems that are in place where the corporation's information security controls have failed.

Procedural breaches are those in which the corporation mishandled the data. These breaches are characterized by the loss of data through mailings a.k.a. "snail mail", publically accessible information on the corporate web site, or improper disposal of records.

HYPOTHESES

Based on the discussion above, it is clear that there are many facets to the problem of securing public information. One of the central debates, however, addresses the appropriate role of government in the information security space. There is a tension between the requirements for market efficiency and national security / privacy. In order to determine the appropriate public policy response, it is necessary to first determine if the market is regulating itself. The following analysis is focused on determining if the market is imposing any punishment on corporations that suffer data breaches and, if so, does that punishment vary across data breach types. This

study expands considerably the dataset used for an analysis of stock price impact in the time period around a data breach announcement. In addition, it looks at not just the change in the stock price but also accounts for the direction of the market index.

HYPOTHESIS 0: BREACHED COMPANIES SUFFER A NEGATIVE STOCK PRICE IMPACT

Using a new and expanded data set, this hypothesis attempts to replicate previous findings showing a small negative impact.

HYPOTHESIS 1: STOCK PRICE IMPACT DIFFERS ACROSS BREACH TYPES

As mentioned above, there are many ways for a company to lose data. With the moves toward and, in some cases, requirements for developing an information security management system, one might expect that the breaches that are more easily addressed by an information security management system may show a more significant stock price impact.

HYPOTHESIS 2: NUMBER OF RECORDS LOST DIFFERS ACROSS BREACH TYPES

Due to the nature of the breaches in each breach type, a difference in the number of records lost is expected. One might expect that Physical breaches where hardware such as backup tapes are lost, to result in many more lost records than a breach where documents were disposed of improperly.

HYPOSTHESIS 3: STOCK PRICE IMPACT IS CORERLATED WITH THE NUMBER OF RECORDS LOST

Similar to checking for differing stock price impact across data breach types, this hypothesis proffers a correlation between stock price impact and the number of records lost. This is an important test to see if the market is making progress toward self-regulating to limit the number of records lost.

HYPOTHESIS 4: MORE RECENT BREACHES SHOW A GREATER STOCK PRICE IMPACT

As outlined above, both the public and private sector are increasingly aware of the risks to information. This hypothesis tests to see if the more recent data breaches, where media attention has been greater, show a more significant stock price impact than earlier breaches.

HYPOTHESIS 5: THE NUMBER OF RECORDS LOST IS DROPPING OVER TIME

Another result of the increasing attention paid to data loss incidents both in terms of media attention and concerted policy efforts by both public officials and corporations should be the reduction in amount of private data lost over time.

CHAPTER 3 – METHODOLOGY

This study investigates multiple hypotheses regarding data breaches. The critical variables collected and their sources are shown in Table 1. A complete list of the variables used including explanations can be found in the codebook in the appendix.

Critical Variables	
Variable	**Source**
Incident Date	datalossdb
Breach Type	datalossdb
Number of Records Lost	datalossdb
Company	datalossdb
Ticker Symbol	EODData
Index	EODData
Stock Price Day 0	EODData
Stock Price Day -3	EODData
Stock Price Day +3	EODData
Index Price Day 0	EODData
Index Price Day -3	EODData
Index Price Day +3	EODData

Table 1: Critical variables in the analysis

SAMPLING PROCEDURES

Whereas existing studies have sampled data breach incidents based by either picking the top results from a query to the Lexis Nexus periodical database (Smith, Smith, & Smith, 2011) , statistically, this project was more statistically rigorous. Data breach incident data was downloaded from the data loss incident database at datalossdb.org[1]. This open source

[1] Datalossdb.org previously provided a tool that allowed for the complete database to be downloaded as a csv file but this is no longer the case. The data for this study was downloaded without headers from

database draws relies on volunteers to transcribe data breach announcements released by the relevant authorities in each of the 48 states that currently have data breach notification laws. The complete list of sources that datalossdb draws on is listed in the appendix.

The loss incidence data included information on 5005 incidents of which 3355 incidents contained data on the number of records lost. Of those, 2682 incidents were incidents in the United States and 1090 involved businesses. Incidents with the breach type "Unknown" were deleted resulting in 1081 incidents. Due to the limited date range of the stock price data, incidents before 1/1/2000 were excluded. The resulting incident dataset included information on 1023 incidents.

The datalossdb data used a different breach classification scheme than that used in this analysis. The datalossdb incident data was consolidated from the 25 category scheme provided to a 3 category scheme which includes three breach types: Physical, Logical, and Procedural. The counts (N) for the new scheme are shown in Table 2[2] below.

Data Breach Categories	
Physical	388
Logical	499
Procedural	136

Table 2: Re-categorized incident counts

---

http://datalossdb.org/exports/dataloss.csv on 2/26/2012. Similar data can be accessed through other sources such as Privacy Rights Clearing House.

[2] See the appendix for the complete list of the datalossdb breach categories with explanations and a table showing the mapping between the datalossdb scheme and the scheme used here.

The stock price and index data was collected from a commercial source called EODData[3]. The end of day stock price data was captured for all stocks traded on both the New York Stock Exchange (NYSE) and the NASDAQ Exchange for from January 1, 2000 through April 22, 2012.

The data loss incident data was loaded into an SQL database and a stratified sample was taken by requesting 100 randomly selected incidents for each of the lower level breach types. A representative SQL query for the "Documents" breach type is shown below:

```
SELECT * FROM `datalossdb` WHERE `New Breach Type Lower` = 'Documents'
ORDER BY RAND() LIMIT 0,100
```

The resulting incident data were checked row by row to see if the business involved in the data breach was a publically traded organization. If the incident involved a corporation that was publically traded on the NYSE or NASDAQ at the time of the breach, the ticker symbol was retrieved using internet searches of the NYSE, NASDAQ, and Google Finance databases. If the business was not publically traded, the row was discarded. This process was continued until sticker symbols were associated with at least 20 incidents for each of the lower level breach types. Note that, due to a limited number of data loss incidents on record, only 4 incidents were included for the "Documents" breach type.

With the incidents matched with stock ticker symbols, the stock price information was retrieved from the historical stock price information. Stock price information was collected for the corporation on the day of the data breach announcement, 3 trading days prior to the announcement, and 3 trading days after the announcement. In addition, the stock market index prices were collected for the same dates. The indices used were "NYA" for the New York Stock Exchange and "COMP" for the NASDAQ exchange.

---

[3] Due to licensing agreements, the author may not be able to release the completed data used in this study as it includes this pay for access data.

ANALYTICAL METHOD

The statistical analysis performed in this research was a series of across-groups ANOVA tests. For each hypothesis, groups were defined and an ANOVA was conducted to test for significant differences in the dependent variable across the groups.

While variables used in the analysis of each hypothesis is outlined below, is it necessary to mention that each of the variables was inspected and transformed as necessary to ensure the normal distribution necessary for ANOVA. Where necessary, the results are described in both transformed and untransformed values.

The dependent stock price impact variable used in several of the hypotheses was calculated using the equations shown below.

$$\%\ Stock\ Price\ Change = \left(\frac{Stock\ Price\ t_0}{Stock\ Price\ t_1} * 100\right) - 100$$

$$\%\ Index\ Price\ Change = \left(\frac{Index\ Price\ t_0}{Index\ Price\ t_1} * 100\right) - 100$$

$$Stock\ Price\ Impact = \frac{\%\ Stock\ Price\ Change - \%\ Index\ Price\ Change}{|\%\ Index\ Price\ Change|}$$

Where the stock impact is being measured in the analysis, the dependent variable was measured against 3 different independent "impact time frame variables" that measure the stock price impact over 3 time periods:

- 3 days prior to the breach through 3 days following the breach (-3 days to +3 days)
- 3 days prior to the breach through the day of the breach (-3 to day 0)
- The day of the breach through 3 days following the breach (day 0 to +3 days)

CHAPTER 4 – RESULTS AND DISCUSSION

HYPOTHESIS 0: BREACHED COMPANIES SUFFER A NEGATIVE STOCK PRICE IMPACT

H_0: There is no difference between the index price and stock price

H_a: There is a difference between the index prices and stock price

Paired sample t test conducted to check for a significant difference in means between the stock price impact and the index price impact across the 3 impact time frame variables. The only significant difference was found in -3 days to day 0, $t(104) = -1.99$, $p = .049$. The mean stock price change was 0.39% and the mean index price change was 1.04%. Overall, the difference between these means was negative (-.65%) and statistically significant negative.

HYPOTHESIS 1: STOCK PRICE IMPACT DIFFERS ACROSS BREACH TYPES

H_0: There is no difference in stock price impact across breach types

H_a: There is a difference in stock price impact across breach types

Independent Variable: Breach Type

Dependent Variable: Stock Price Impact Time Frame

The ANOVA results were computed for the 3 impact time frame variables. A significant impact difference was found in the -3 days to +3 days time frame ($F(2,106) = 3.672$, $p = .029$). A Tukey HSD post-hoc test shows the difference in stock price impact between the Logical breach type and the Procedural breach type with mean impacts of -2.32% and .728% respectively.

In addition, a significant difference was found in the day 0 to +3 days time frame ($F(2,107) = 3.871$, $p = .024$). A Tukey HSD post-hoc test shows the significant difference is again between the Logical breach type and Procedural with mean impacts of -1.64% and 1.22% respectively.

HYPOTHESIS 2: THE NUMBER OF RECORDS LOST DIFFERS ACROSS BREACH TYPES

H_0: There is no difference in number of records lost across breach types

H_a: There is a difference in number of records lost across breach types

Independent Variable: Breach Type

Dependent Variable: Number of Records Lost

An ANOVA of the upper level breach categories shows a significant difference in the number of records lost across the upper level breach categories ($F(2,111) = 4.036$, $p = 0.020$). A Tukey HSD post-hoc analysis shows significant differences between the following Physical and Procedural breach categories with untransformed means of 8916 records and 916 records respectively. The complete results are shown in the table below.

Records Lost Across Breach Types		
Breach Type	**Transformed Mean**	**Untransformed Mean**
Physical	3.95	8916
Logical	3.67	4638
Procedural	2.96	916

Table 3: Mean Number of Records Lost Across Breach Types

HYPOTHESIS 3: STOCK PRICE IMPACT IS CORRELATED WITH THE NUMBER OF RECORDS LOST

Pearson's correlation was calculated for the three impact time frame variables and the number of records lost variable. No statistically significant correlation was found.

HYPOTHESIS 4: MORE RECENT BREACHES SHOW A GREATER STOCK PRICE IMPACT

H_0: There is no difference in stock price impact for more recent events

H_a: There is a difference in stock price impact for more recent events

Independent Variable: Time Period

Dependent Variable: Stock Price Impact Time Frame

The incident database was split into three groups. One group contained incidents from the start through December 31, 2006 (N = 35), another contained January 1, 2007 through December 31, 2009 (N = 45), and the last contained events from January 1, 2010 through the end of the database (N = 34).

An ANOVA across the three time periods for each of the impact time frame variables found a significant difference only in the day 0 days to +3 days time frame ($F(2,107) = 4.105$, $p = .019$). The mean impact is shown in Table 4.

Stock Price Impact Over Time	
Time Period	**Mean Impact**
July 5, 2001 - December 31, 2006	0.35%
January 1, 2007 - December 31, 2008	-1.88%
January 1, 2009 - January 26, 2012	0.22%

Table 4: Mean Stock Price Impact Over Time

HYPOTHESIS 5: THE NUMBER OF RECORDS LOST IS DROPPING OVER TIME

H_0: There is no difference in the number of records lost for more recent events

H_a: There is a difference in the number of records lost for more recent events

Independent Variable: Time Period

Dependent Variable: Number of Records Lost

The incident database was split into three groups. One group contained incidents from the start through December 31, 2006 (N = 35), another contained January 1, 2007 through December 31, 2009 (N = 59), and the last contained events from January 1, 2010 through the end of the database on January 26, 2012 (N = 18).

An ANOVA across the three groups did not show significant difference in records lost over time. However, the mean values are noteworthy and are summarized in the table below.

Records Lost Over Time		
Time Period	**Mean Records Lost Transformed**	**Mean Records Lost Untransformed**
July 5, 2001 - December 31, 2006	3.914	8204
January 1, 2007 - December 31, 2009	3.418	2618
January 1, 2010 - January 26, 2012	3.281	1909

Table 4: Mean Stock Price Impact Over Time

DISCUSSION

This analysis shows that there is a significant difference between the mean index price change and the mean stock price change in the dataset. This data included only breached companies so we would expect that the stock price change would be less than the index price change in accordance with previous research. This is confirmed by the data that show the mean stock price change was 0.39% whereas the mean index price change was 1.04%.
The significant stock price impact found between the Logical and Procedural breach types with respective means of -2.32% and .728% respectively further confirm that there is a significant amount of noise in the data since it seems strange that a data breach of any type may result in a positive stock price impact. The negative impact as a result of the Logical breaches may be an indication that the market that is becoming aware of the need for robust information security management systems, is punishing companies that implement those systems poorly.

From the perspective of aligning market punishment with the loss of public information, it is troubling that no correlation was found between stock price impact and the number of records lost. This indicates that the market is not aware of or simply not responding to differing scales of lost information. The stock price impact over time, however, may be trending downward. In order from the earliest group of breaches to the most recent, the stock price impact varies from 0.35%, -1.88%, to 0.22%. Again it is strange to see the impact of a breach being positive but it is important to note that, while inconsistent in slope, the stock price impact is trending downward. This may mean that the increasing attention being paid to data breaches is having a small effect in the market.

When considering public or corporate initiatives to limit the amount of public information being lost, this analysis provides some direction. As expected, the Physical data breaches result in significantly more records being lost at a mean of 8916 records per incident whereas Procedural breaches result in a mean of 916 records lost per incident. With an increasingly mobile workforce it may be difficult to legislate that companies stop losing physical assets to

theft or loss but there may be an opportunity to limit the number of records kept on mobile hardware. In all, though, the controls put in place over the past decade to control information loss do seem to be having an impact (although not statistically significant) on the mean number of records lost per incident which has dropped from 8204 to 1909.

CHAPTER 5 – CONCLUSION

LIMITATIONS

This study is limited in both time and geography. The stock price data was limited to starting in the year 2000. This did not impact the analysis much because there were only few data breach incidents in the database before January 1, 2000. However, the data breach notification laws have been gradually introduced over the time frame covered so it is possible that there were incidents that are not included because there was no notification requirement in place at the time. The source incident data is provided by state level authorities and that means that incidents are only entered in the database if the state has a data breach notification law and the corporation knew about the breach and chose to report it. Companies have many incentives to choose not to release information on a data breach. Even with data breach notification laws in place in most states, the available data on breaches may be skewed because companies are only reporting what they have to rather than reporting every incident. In addition, the reliance on state level sources means that the incident data is limited to the United States.

FUTURE RESEARCH

Considering that the data breach notification laws are now in place in almost every state and data breach announcements are becoming an almost daily event, this study might yield different results if repeated. The most time consuming portion of the study was to collate the datalossdb data with the stock price information. Even with the existing sources, it may be possible to automate this routine to limit the amount of data entry time required. A better approach, however, would be to have an official data breach announcement broker that is open to manipulating the way data breach information is tabulated to ease the workload on researchers. This would be as easy as adding a dichotomous variable for publically traded and a text variable for ticker symbol in the data breach incident data.

This study did not exhaust the analysis possible with the datalossdb incident data. One possible study would look at the stock price impact numbers across the various types of customer data lost. A 2012 study shows that corporate leaders prioritize protecting customer data over employee data or intellectual property.

SUMMARY

This study expands the data set and adds some measure of statistical rigor to previous studies that have looked for stock price impact around data breach announcements. This study found a downward trend in the stock price around the time of a data breach. While the market does seem to be distinguishing between certain breach types, no correlation was found between the stock price and the number of records lost. This suggests that although the market may be self-regulating, the punishments are not consistent with volume of lost private information. On a more positive note, the regulations being implemented by public authorities and the controls being implemented inside organizations are reducing the number of records lost over time. Taken together, the results of this study show that there is a need for better information in the marketplace. The two common reasons for government intervention in the market are efficiency and equity. The market for information security seems to be on the road toward self-regulation but, with the rising tide of threats to information security, the government could push the process forward by developing information sharing centers where corporations and governments can share breach information.

BIBLIOGRAPHY

Alexander, P. (2007, April 9). Data breach notification laws: A state-by-state perspective. *Information Week*.

Andoh-Baidoo, F., & Osei-Bryson, K.-M. (2007). Exploring the characteristics of internet security breaches that impact the market value of breached firms. *Expert Systems wit Applications*, 709-725.

ASIS Foundation. (2002). *Trends in proprietary information loss.* ASIS Foundation.

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology*.

Birkland, T. (2005). *An introduction to the policy process: Theories, concepts, and models of public policy making.* Armonk, New York: M.E. Sharpe.

Brennan, J. (2012, April 12). Cybersecurity bills compete for attention. (T. Gjeltan, Interviewer) National Public Radio. 88.5 KPLU, Seattle.

Caldwell, A. (2011, November 28). Feds seize 150 websites in counterfeit crackdown. *USA Today*.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 69-104.

Central Source LLC. (n.d.). *About us*. Retrieved June 1, 2012, from AnnualCreditReport.com: https://www.annualcreditreport.com/cra/helpabout

Cerdes, L. (Ed.). (2009). *Cyber Crime.* Detroit, MI: Greenhaven Press.

Clough, J. (2010). *Principles of Cybercrime.* New York: Cambridge University Press.

Computer Security Division. (n.d.). *Computer security resource center special publications*. Retrieved May 21, 2012, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/PubsSPs.html

Computer Weekly. (2010, April 20). *UN rejects international cybercrime treaty.* Retrieved from http://www.computerweekly.com/Articles/2010/04/20/240973/UN-rejects-international-cybercrime-treaty.htm

Covielo, A. (n.d.). *Open letter to RSA customers*. Retrieved December 9, 2011, from RSA: http://www.rsa.com/node.aspx?id=3872

Curtin, C., & Ayers, L. T. (2009). Using science to combat data loss: Analyzing breaches by type and industry. *A Journal of Law & Policy for the Information Society*.

Dunham, K. (2012, Februrary). Top cyber threats for 2012. *ISSA Journal*, p. 47.

Endicott-Popovsky, P. B. (2011). IMT 551 course lecture.

Engineering Information Institute. (2011, November 29). *Researchers explore how cyber-attackers think like regular crooks.* Retrieved April 28, 2012, from University of Maryland: http://eit.umd.edu/html/news/news_story.php?id=6141

Federal Trade Commision. (2006, November 6). *Data security and privacy considerations*. Retrieved May 20, 2012, from Protecting consumers in the next tech-ade: http://www.ftc.gov/bcp/workshops/techade/data.html

Goel, S., & Shawky, H. (2009). Estimating the market impact of security breach announcements on firm values. *Information and Management*.

Gruber, J. (2011). *Public Finance and Public Policy.* New York: Worth Publishers.

Infragard. (n.d.). *InfraGard - public private partnership - Federal Bureau of Investigation*. Retrieved December 1, 2011, from Infragard: http://www.infragard.net/

ISC2. (n.d.). *ISC2*. Retrieved December 9, 2011, from ISC2: https://www.isc2.org/

ISSA. (n.d.). *Welcome to ISSA.org*. Retrieved November 15, 2011, from Information Systems Security Association (ISSA): https://www.issa.org/

Jackson, W. (2012, April 27). *House wraps up cyber week by passing two more security bills*. Retrieved May 20, 2012, from Government Computer News: http://gcn.com/Articles/2012/04/27/House-passes-more-cyber-bills.aspx?Page=2

Jaishankar, K. (Ed.). (2011). *Cyber criminology: exploring internet crimes.* Boca Raton, Florida: CRC Press.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, 69-91.

Kizza, J. M. (2009). A guide to computer network security. In J. M. Kizza, *Security Beyond Computer Networks: Information Assurance* (pp. 449-453). New York: Springer.

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, 541-562.

Lipner, S., & Howard, M. (2005, March). *The trustworthy computing security development lifecycle*. Retrieved December 9, 2011, from msdn: http://msdn.microsoft.com/en-us/library/ms995349.aspx

Marsan, C. D. (2012, May 3). Hottest IT skill? cybersecurity. *PC World*.

Montagne, R. (2011, November 29). Following digital breadcrumbs to 'big data' gold. Retrieved from http://www.npr.org/templates/transcript/transcript.php?storyId=142521910

Moyle, E., & Kelley, D. (2012, April 23). Federal IT survey: Hacktivists, cybercriminals are top threats. *Information Week*.

Obama, B. (2011). *International strategy for cyberspace.* Washington: The White House.

Office of Information Technology. (n.d.). *Definition of information security*. Retrieved May 31, 2012, from University of Nevada, Las Vegas: http://oit.unlv.edu/network-and-security/definition-information-security

Office of the Assistant Secretary of Defense (Public Affairs). (2012, May 11). *DOD announces the expansion of defense industrial base (DIB) voluntary cybersecurity information sharing activities.* Retrieved May 27, 2012, from U.S. Department of Defense: http://www.defense.gov/releases/release.aspx?releaseid=15266

Open Web Application Security Project. (n.d.). *Top 10 2010-main*. Retrieved December 8, 2011, from OWASP: https://www.owasp.org/index.php/Top_10_2010-Main

Picanso, K. E. (2006). Protecting information under a uniform data breach security notification law. *Fordham Law Review*, 355-390.

Pierson, C. (2011). SecureWorld conference lunch keynote.

Radia, R. (2012, April 21). *Free market coalition letter on CISPA.* Retrieved June 1, 2012, from Competetive Enterprise Institute: http://cei.org/coalition-letters/free-market-coalition-letter-cispa

Roberds, W., & Schreft, S. L. (2009). Data security, privacy, and identity theft: The economics behind the policy debates. *Economic Perspectives, 33*(1).

Rubin, P. H., & Lenerd, T. M. (2005). *An economic analysis of notification requirements for data security breaches.* Washington, D.C.: The Progress and Freedom Foundation.

Schreft, S. L. (2007). Risks of identity theft: can the market protect the payment system? *Economic Review*, 5-40.

Schrier, R. (2011). US CYBERCOM and Cybersecurity Lecture Film. (G. W. University, Interviewer)

Smith, K. B., & Larimer, C. W. (2009). *The public policy theory primer.* Boulder: Westview Press.

Smith, K., Smith, L. M., & Smith, J. L. (2011). Case Studies of cybercrime and its impact on marketing activity and shareholder value. *Academy of Marketing Studies*.

Subramani, M., & Walden, E. (2001). The Impact of e-commerce announcements on the market value of firms. *Information System Research*, 135-154.

Sullivan, E. (2012, April 17). Ex FBI cyber cop takes job with startup company. *The Seattle Times*.

Swire, P. (2003). Efficient confidentiality for privacy. In R. Herring, & R. E. Litan (Eds.), *Brookings–Wharton Papers on Financial Services* (pp. 273-310). Washington, D.C.: Brookings Institution Press.

Tipton, H. F. (Ed.). (2010). *Official (ISC)2 guide to the cissp cbk* (2 ed.). Boca Raton, FL: Auerbach Publications.

U.S. Department of Health and Human Services. (n.d.). *Breach notification rule*. Retrieved May 31, 2012, from U.S. Department of Health and Human Services: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

United States Computer Emergency Readiness Team. (n.d.). *Cyber security tip ST04-014*. Retrieved December 9, 2011, from National Cyber Alert System: http://www.us-cert.gov/cas/tips/ST04-014.html

Wolf, J. (2012, April 24). U.S. eyes broader cyber-threat pact with companies. *Chicago Tribune*.

Wong, K. M. (2011, September 28). *Moving (slowly) toward a national data breach notification standard*. Retrieved December 9, 2011, from Data Breach Legal Watch: http://www.databreachlegalwatch.com/2011/09/moving-slowly-toward-a-national-data-breach-notification-standard/)

APPENDIX A: DEFINITIONS OF KEY TERMS

Cybercrime: "The range of technology-enabled crime is always evolving, both as a function of technological change and in terms of social interaction with new technologies" (Clough, 2010, p. 8)

Hacking: The act of gaining unauthorized access to computers and computer systems. Described by the Cybercrime Convention as, "offences against the confidentiality, integrity, and availability of computer data and systems" (Clough, p. 27)

Data: While the laws addressing cybercrime define data as "information in any form" (Clough, p. 61) this project is concerned with data that allows for the identification of individuals. This information is known as Personally Identifiable Information.

Personally Identifiable Information (PII): "any piece of information that could be used to uniquely identify a person. This includes but is not limited to a person's name, address, phone number, birth date, social security number, or credit card and bank account numbers." (Federal Trade Commision, 2006)

Data Breach: "A breach is, generally, an impermissible use or disclosure…that compromises the security or privacy of the protected…information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual." (U.S. Department of Health and Human Services)

Information Security Management System (ISMS): "The governance structure supporting an information security program" (Tipton, 2010, p. 679)

Information Security: "as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and

against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats." (Office of Information Technology)

APPENDIX B: DATALOSSDB CATEGORIES AND DESCRIPTIONS[4]

Breach Types	
Short Name	**Description**
Disposal Computer	Discovery of computers not disposed of properly
Disposal Document	Discovery of documents not disposed of properly
Disposal Tape	Discovery of backup tapes not disposed of properly
Disposal Drive	Discovery of disk drives not disposed of properly
Disposal Mobile	Discovery of data on a mobile phone or device such as tablets, etc
Email	Email communication exposed to unintended third party
Fax	Fax communication exposed to unintended third party
Fraud Se	Fraud or scam (usually insider-related), social engineering
Hack	Computer-based intrusion, data not generally publically exposed
Lost Computer	Lost computer (unspecified type in media reports)
Lost Document	Discovery of documents not disposed of properly through loss (not theft)
Lost Drive	Lost data drive, unspecified if IDE, SCSI, thumb drive, etc)
Lost Laptop	Lost laptop (generally specified as a laptop in media reports)
Lost Media	Media (i.e. disks) reported to have been lost by a third party
Lost Mobile	Lost mobile phone or device such as tablets, etc (unspecified in media reports)
Lost Tape	Lost backup tapes
Missing Document	Missing document, unknown or disputed whether lost or stolen
Missing Laptop	Missing laptop, unknown or disputed whether lost or stolen
Missing Media	Missing media, unknown or disputed whether lost or stolen
Snail Mail	Personal information in "snail mail" exposed to unintended third party
Stolen Computer	Stolen desktop (or unspecified computer type in media reports)
Stolen Document	Documents either reported or known to have been stolen by a third party
Stolen Drive	Stolen data drive, unspecified if IDE, SCSI, thumb drive, etc)

[4] http://datalossdb.org/analysis

Stolen Laptop	Stolen Laptop (generally specified as a laptop in media reports)
Stolen Media	Media (disks or other) generally reported or known to have been stolen by a third party
Stolen Mobile	Stolen mobile phone or device such as tablets, etc
Stolen Tape	Stolen backup tapes
Unknown	Unknown or unreported breach type
Virus	Exposure to personal information via virus or trojan (i.e. keystroke logger, possibly classified as hack)
Web	Computer/web-based intrusion, data typically available to the general public via search engines, public pages, etc.

Data Types	
Short Name	**Description**
CCN	Credit Card Numbers
SSN	Social Security Numbers (or Non-US Equivalent)
NAA	Names
EMA	Email Addresses
MISC	Miscellaneous
MED	Medical
ACC	Account Information
DOB	Date of Birth
FIN	Financial Information
UNK	Unknown
PWD	Passwords
ADD	Addresses

Sectors / Business Types	
Short Name	**Description**
Biz	Business
Edu	Educational
Gov	Government
Med	Medical

Sector / Business Sub-Types	
Short Name	**Description**
Retail	Retail Businesses
Fin	Financial
Tech	Technology
Med	Medical (Non-Hospital / Provider)
Fed	Federal Government
Data	Data Services / Brokerage
Media	Mass Media
Uni	University
Ind	Industry
State	State Government
NFP	Non-Profit / Not-For-Profit
County	County Government
Org	Organization
Hos	Hospital
HS	High School
Ins	Insurance
City	City (Government or Citizens)
Hotel	Hotel
Law	Legal Firm
Elem	Elementary School
Edu	Educational
Biz	Business
Gov	Government
Pro	Medical Provider
Agr	Agricultural

APPENDIX C: DATA INCIDENT RECATEGORIZATION

The table below shows the original count of incidents from the datalossdb database.

Datalossdb count	
Type of Incident	**Number of Incidents**
Disposal Computer	4
Disposal Document	29
Disposal Drive	1
Disposal Tape	1
Email	40
FraudSe	156
Hack	240
Lost Computer	4
Lost Document	16
Lost Drive	11
Lost Laptop	9
Lost Media	21
Lost Tape	25
Missing Laptop	1
Missing Media	1
Snail Mail	45
Stolen Computer	60
Stolen Document	28
Stolen Drive	9
Stolen Laptop	201
Stolen Media	5
Stolen Mobile	2

Stolen Tape	11
Virus	14
Web	89

The table below shows the re-categorization to the scheme used in this analysis.

Breach Type Re-categorization Key	
Datalossdb Breach Type	**Curtin and Ayers Breach Type**
Disposal Computer	Procedural
Disposal Document	Procedural
Disposal Drive	Procedural
Disposal Tape	Procedural
Lost Computer	Physical
Lost Document	Physical
Lost Drive	Physical
Lost Laptop	Physical
Lost Media	Physical
Lost Tape	Physical
Missing Laptop	Physical
Missing Media	Physical
Snail Mail	Physical
Stolen Computer	Physical
Stolen Document	Physical
Stolen Drive	Physical
Stolen Laptop	Physical
Stolen Media	Physical
Stolen Mobile	Physical
Stolen Tape	Physical
Virus	Logical
Web	Procedural
Email	Logical
FraudSe	Logical
Hack	Logical