

SECURITY BREACH DISCLOSURE

SECURITY BREACH DISCLOSURE

By Yao-Tien Lee, B.Sc., M.Sc., M.B.A.,

A Thesis Submitted to the School of Graduate Studies in Partial Fulfillment of the
Requirement for the Degree Ph.D. in Business Administration

McMaster University © Copyright by Yao Tien Lee, August, 2018

Ph.D. in Business Administration (2018)

McMaster University

Information Systems

Hamilton, Ontario

TITLE: Security Breach Disclosure

SUPERVISOR: Dr. Yufei Yuan

Number of Pages: 203

Lay Abstract

Recent cases of security breach at Equifax, Yahoo, and Uber have raised attention from the public and regulators on the issues of public disclosure of security incidents. However, the lack of understanding and research in security breach disclosures has hampered our ability in defining what needs to be disclosed, understanding what are actually disclosed, and determining how well the incidents are disclosed. These issues are urgent and important thus warrant considerable efforts to carefully examine the current landscape of policy and practice, and to provide methods to evaluate disclosures so that meaningful advancements in research and improvements in practice can be made. This study recommends a set of core elements in disclosure, develops methods to extract information from disclosure, establishes ways to evaluate quality, and proposes a framework that maps out future research. These are important advancements in the study of security breach disclosure and will contribute greatly towards future policies, practice, and research.

Abstract

Security breach disclosure is the public disclosure of information regarding a data security incident. It allows organizations to communicate salient information to the affected parties and stakeholders regarding the nature and impact of the breach, and remediating solutions undertaken regarding the breach. Recent cases of large-scale security breaches have revealed that security breach disclosure remains a challenging subject for policymakers, practitioners, and researchers. There is a lack of understanding and consensus on what breaches need to be disclosed and little evidence on how actual practices are employed.

Using an adapted grounded theory methodology that combines computerized textual extraction and ground theory coding techniques, this study explores relevant issues through four research questions with distinct objectives that would enhance understanding of the issues in public breach disclosure. First, recent regulations from the US, EU, and Canada are reviewed to identify the core elements in breach disclosure. Second, this study develops methods to extract information content from disclosures. Third, matrices and measuring instruments are developed to evaluate the quality, and last, a framework is proposed to map out the paths and directions for future research. These advancements lay the crucial groundwork in the field of security breach disclosure and will contribute greatly towards future policies, practice, and research.

The expected societal significance of this research is profound. The research is relevant to practitioners, regulators, and the information security community as it provides valuable insight on current challenges and future directions. The ultimate goal is to strengthen our understanding of security breach disclosure and enhance the accumulation and transfer of knowledge obtained through security breach disclosure; thereby providing organizations, regulators, and the information security community with the information necessary to develop policies, tools, and controls for identifying, managing, and reducing the risks of future security incidents. The proposed core elements, methods of extracting relevant information content, quality evaluation matrices, and framework mark a significant advancement towards this vision.

Acknowledgement

This work would not have been possible without the supervision, support, and commitment from my Dissertation Committee. I am especially indebted to Dr. Yufei Yuan, Professor of the Information Systems Department who has been supportive of my study from the very first day that I set in his office discussing my goals in the Ph.D. Program.

I am grateful to all of those with whom I have had the pleasure to work during my years in the Ph.D. Program. Particularly, I am honored to be advised by three very distinguish scholars in McMaster University, Dr. Yufei Yuan, Dr. Norm Archer, and Dr. Jiaping Qiu. Each of the members of my Dissertation Committee has provided me extensive personal and professional guidance and taught me a great deal about both scientific research and life in general. It is an exquisite privilege to be able to work with them.

I would especially like to thank Dr. Yufei Yuan, the chairman of my committee. As my teacher and mentor, he has taught me more than I could ever give him credit for here. He has shown me, by his example, what a good scientist (and person) should be. Dr. Yuan's patience and tolerance in helping me understanding my shortcomings and his wonderful encouragement in strengthening my confidence in leveraging my experience from my work have made this difficult journey ever so enjoyable.

I would also like to thank my external reviewer, Dr. Francine Vachon, her enthusiasm and professionalism during the review process and her wonderful comments during the final examination have further invigorated my passion towards the field of research.

Nobody has been more important to me in the pursuit of this project than the members of my family. I wish to thank my loving and supportive wife, Chinatsu, and my three wonderful children, Ethan, Amber, and Avery, who provide unending motivation.

TABLE OF CONTENTS

1	Introduction	1
1.1	Research Premise	1
1.2	Research Motivation & Rationale	6
1.3	Research Questions	11
1.4	Research Objective	15
1.5	Research Approach	18
1.6	Summary	20
2	The essential facets of security breach & breach disclosure	23
2.1	From Security Incident to External Breach Disclosure	23
2.2	Review of Current State of Research	29
2.3	Review of Current Practices of Breach Disclosure	35
2.4	Review of the Current State of Policies	50
2.5	Summary	58
3	Theory and Conceptual Background	59
3.1	The Economics of Disclosure	59
3.2	Mandatory Disclosure	60
3.3	Voluntary Disclosure	63

3.4	Management Discretion and Control of Disclosure.....	64
4	The Elements of Security Breach Disclosure Requirements (RQ1).....	67
4.1	Common principles and provisions for disclosure.....	67
4.2	Methodology	71
4.3	Elements of Security Breach Disclosure.....	78
4.4	Usage Example of the Common Elements.....	85
4.5	Summary	86
5	The Information Content of Security Breach Disclosure (RQ2).....	88
5.1	Extracting Information Content from Unstructured Breach Reports.....	88
5.2	Extraction Approach	89
5.3	Data Source	91
5.4	Methodology	93
5.5	Descriptive Analysis	99
5.6	Analysis of what are contained in breach disclosures.....	104
5.7	Summary	110
6	Evaluating Security Breach Disclosure (RQ3).....	112
6.1	Quality Domains & Measuring Instruments of Disclosure.....	112
6.2	Methodology	115
6.3	Evaluation Results.....	125

6.4	Analysis.....	129
6.5	Factors that Affect Disclosure Scores	132
6.6	Summary	138
7	Security Breach Disclosure Framework.....	139
7.1	Security Breach Disclosure Framework.....	139
7.2	Use of the Framework and Future Research Directions	141
7.3	Management Discretion and Disclosure Practices	142
7.4	Information Security Community and Knowledge Building for ISM	143
7.5	Summary	145
8	Conclusions	147
8.1	Discussion of Major Findings	147
8.2	Research Significance & Contribution.....	154
8.3	Recommendations towards Better Breach Disclosure Practices.....	158
8.4	Threat Information Sharing through Disclosure	161

LIST OF FIGURES AND TABLES

Table 1-1: Summary of Research Questions, Focus, Objective, Approach, and Output...	21
Figure 2-1: From Security Incidents to Publicly Disclosed Security Breach	29
Figure 2-2: Example of a Customer notification from Home Depot (Page 1/3)	39
Figure 2-3. Example of Vulnerability Disclosure collected by CERT	43, 44
Table 2-1: Summary of Current Breach Disclosure Practices	48
Figure 4-1: GTM Coding Processes	71
Figure 4-2: Common Elements of Security Breach Disclosure.....	76
Table 5-1 Research Concerns in Using Human vs Computer for Knowledge Extraction.	87
Figure 5-1: A Visualization of Part of Speech Tagging and Syntactic Dependency Information from a Breach Disclosure	91
Figure 5-2 Breach Disclosure XML Document Base Structure	94
Figure 5-3 Expanded Disclosure XML Example.....	95
Table 5-2: Breach Report Properties by Year (2012-2016).....	96
Figure 5-4 Fit Plot for Number of Disclosure Reports	97
Figure 5-5 Fit Plot for Number of Disclosure Delay	98
Table 5-3: Breach Report Properties by Industry	100

Table 5-4 Breach Report Common Elements	101
Figure 5-6 Disclosure Coverage of Common Elements	102
Table 5-5 Percentage of Ambiguous Reporting.....	105
Figure 6-1: Timeliness Issues for Security Breach Disclosure.....	112
Table 6-1 Example of a Detailed Report with Multiple Time References	116
Table 6-2 Example of Disclosure with Little Management Oversight	118
Table 6-3: Threat Agent Identification – External Agents	120
Table 6-4: Composite Scores of Completeness, Time References, and Management Involvement	121
Table 6-5 Composite Score by Year	122
Figure 6-2: Fit Plot for Report Completeness in Security Disclosure from 2012 to 2016	123
Figure 6-3: Fit Plot for Management Involvement (mgnt_inv) in Security Disclosure from 2012 to 2016	124
Table 6-6 Composite Score by industry.....	125
Table 6-7 Evaluation Score Pearson / Spearman correlation.....	127
Table 6-8 Variable Description.....	129
Table 6-9 General Leastsquares Model with Fixed Effect Results.....	133
Figure 7-1: Proposed security breach disclosure framework:.....	140

Table 7-1: Known-unknown Table.:	144
Figure 8-1: California Industry Distribution by Number of Organizations	149

LIST OF ABBREVIATIONS AND ACRONYMS

HIPAA	Health Insurance Portability and Accountability Act
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
GLM	Generalized Least Squares Model
GT	Grounded Theory
GTM	Grounded Theory Method
IASB	International Accounting Standards Board
ICO	Information Commissioner's Office
IS	Information Systems
ISM	Information Security Management
IT	Information Technology
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PIPEDA	Protection and Electronic Document Act
SOX	Sarbanes-Oxley Act
XML	Extensible Markup Language

SECURITY BREACH DISCLOSURE

“Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants”
- Justice Louis D. Brandeis

1 Introduction

1.1 Research Premise

On September 7, 2017, Equifax, one of the three largest credit agencies in the world, disclosed that it had suffered a security breach that affected 143 million consumers, one of the worst breaches of all time (Armerding, 2018). The compromised data included social security numbers, full names, addresses, dates of birth, credit card numbers, and other personal information. The potential financial impact on its victims due to possible identity theft is beyond estimate (McCrank & Finkle, 2018). The breach was discovered by Equifax on July 29, 2017 and despite Equifax’s access to resources and potential urgency of the event, Equifax did not make any disclosures either to the public or to its customers until more than forty days after the breach (The Wall Street Journal, 2017).

In addition to the disclosure delays, it was reported that Equifax lobbied for more lax regulation on enforcement of breaches (The Wall Street Journal, 2017); and fought to kill the rule allowing victims to sue (LA Times, 2017). To make matters worse, three

senior executives were reported to have sold Equifax shares worth almost \$1.8 million days after the company discovered the security breach (Bloomberg, 2017). In the wake of the breach, more than 240 class action lawsuits have been filed against the company (Tsukayama, 2017). The United States Congress has subsequently launched an investigation into not only the organization's practices, but also into its CEO's conduct in the "breakdown in security safeguards that led to the company's massive hack" (The Wall Street Journal, 2017). The general public is, understandably, shocked and appalled by the lack of transparency and lack of government oversight over Equifax's action in not disclosing information surrounding the breach and its demands for action from the regulators (Blumenthal & McSweeney, 2017). This security incident uncovered several flaws and highlights our lack of understanding of disclosure regulations and practices. What should be disclosed and to what detail? What is a reasonable timing of disclosure? What are the motivations in delaying disclosure? What are the potential impacts? Perhaps more importantly, can we learn from the mistakes made through disclosures?

The epic failure of Equifax was not the only big event concerning cybersecurity breaches in 2017. On Oct 3, 2017, less than one month after Equifax's news, Yahoo! Inc. amended their prior disclosures and revealed that a security breach back in 2013 had led to compromising all 3 billion of its user accounts (Reuters, 2017). The disclosure practices employed by Yahoo were also very troubling. First, the breach in 2013 was only brought to public attention during its negotiations to sell itself to Verizon in September 2016, a delay of more than three years after the breach. Yahoo disclosed that the attack compromised the real names, email addresses, dates of birth and telephone

numbers of 500 million users (Yahoo! Inc., 2016). However, in December 2016, 3 months after its initial disclosure and 3 years after the incident, Yahoo further disclosed that a separate security breach in 2013, by a different group of hackers, had compromised 1 billion accounts. In addition to names, dates of birth, email addresses, passwords, even security questions and answers were also compromised. The final revelation came on October 3 2017, when Yahoo revised that estimate, admitting that, in fact, all 3 billion user accounts had been compromised (Armerding, 2017). Yahoo's disclosure practice "piecemealed" the news and downplayed its impact. It is difficult to fathom that a technology giant such as Yahoo! Inc. would not be able to conduct a thorough investigation and discover the full extent of the breach. This raises several questions: If Yahoo had disclosed that all 3 billion users accounts were compromised in its first public disclosure, what would have happened to the tech giant? Was it a deliberate act not to fully disclose the breach so as to dampen the potential public backlash? Was an internal disclosure policy actually in place to inform senior management or the company's board of the full extent of the breach?

Although the size of the two breaches at Equifax and Yahoo seem daunting, they are but the tip of the iceberg. The real victims of security breach are seldom the organizations that suffered the attack. The stolen personal data are often collected and sold on the "darkweb" (Ablon et al., 2014). These data could be used as pretext for future attacks on individuals whose data were illegally misappropriated (Ablon et al., 2014). Therefore, as more personal information were breached and made available in the bazaar of organized cybercrime syndicates, more identity-related crime would undoubtedly ensue. Based on

the 2018 Identity Fraud Report by Javelin Strategy & Research (Pascual et al., 2018), there has been a sharp increase in identity theft since 2015. According to the 2017 Ponemon Cost of Data Breach study (Ponemon, 2017), the global average cost of a data breach has reached \$3.62 million per breach.

Recent cases of large-scale cybersecurity breaches have invigorated the discussion of mandatory, enforceable requirements on security breach disclosure (The Wall Street Journal, 2016). Recognizing the importance of security breach disclosure, government agencies and regulators throughout the world have introduced new legal frameworks or accelerated the effort of enforcing regulatory requirements. However, despite policy makers' effort in protecting the public through their continuous call for proper security breach disclosure, the reality of current disclosure practices is alarming and the potential impacts on society are deeply concerning.

From the regulator's perspective, the momentum for stronger cybersecurity breach regulations and guidance to protect the interests of the general public has indeed resulted in codified laws. In the European Union (EU), on April 14, 2016, the General Data Protection Regulation (GDPR) was approved by the EU Parliament with an expected enforcement date of May 25, 2018. GDPR addresses many aspects of information security and privacy considerations. In terms of security breach disclosure, article 33 in GDPR specifies that the "data controller" is under a legal obligation to notify the supervisory authority within a maximum of 72 hours after becoming aware of the data breach. In addition, article 34 specifies that individuals also have to be notified if

adverse impact is determined. In the United States, the Data Security and Breach Notification Act was introduced to the Congress on December 1, 2017. It proposes severe consequences for executives, including jail time, for failing to notify the affected parties of a breach.

For consumers, the stricter penalties for non-compliance may be a long-awaited call, particularly after the discovery of UBER's brazen act in willfully concealing a major security breach for over a year. In November 2017, the new CEO disclosed that UBER paid off hackers in 2016 to hide a breach that affected 57 million users worldwide, including 25 million in the United States (Wong, 2017). Uber's CIO acknowledged that not notifying users was "a mistake" and two employees who handled the response process were subsequently fired (Bensinger & McMillan, 2017). However, UBER's concealment of the breach brought no immediate criminal charge against UBER. The proposed data breach legislation in US would make willful concealment a crime that is punishable by up to five years in prison (Wright, 2017). The bill also states that organization must provide notification to users or customers within 30 days of the discovery of the breach unless a U.S. federal law enforcement or intelligence agency exempts the entity from informing the public.

These recent cases of cybersecurity breaches and organizational disclosure practices have highlighted a process that is far from perfect; our understanding of the policies, requirements, and practices of security breach disclosure are severely lacking. These issues can be analyzed from three main perspectives: 1) from the regulators' perspective,

issues of security breach disclosure include defining what needs to be disclosed, when to disclose, and perhaps more importantly, what protection and rights must be provided to the public through the law. 2) From the organization's perspective, the issues of disclosure practice include what factors and conditions cause organizations to conceal or delay disclosure; to downplay the impact; or, to provide ambiguous, jargon-filled responses. 3) From the academic perspective, recent phenomena have highlighted our lack of understanding in what roles played a hand in security breach disclosures by organizations.

The risk of cybersecurity breaches cannot be completely eliminated; however, there is little excuse for ill-managed breach disclosure practices. Recognizing that there exist significant challenges in terms of policy, practice, and research, this study draws motivation from these challenges.

1.2 Research Motivation & Rationale

Studies in information security management have provided a foundation for compliance behavior (Pahnila et al., 2007; Herath & Rao, 2009; Bulgurcu et al., 2010). Recent advancements in information security research have had a profound impact on our understanding of how individuals take actions to avoid threats (Liang & Xue, 2009; Liang & Xue, 2010) and have explored the paths that lead to security incidents (Ransbotham & Mitra, 2009). For research in security breach disclosure, the majority of studies have focused on the economic consequence of security breaches (Cavusoglu et al., 2004; Kannan et al., 2007; Goel & Shawky 2009; Berezina et al, 2012). Research in this

stream typically employs event study methodology that focuses on stock market reactions post- security incident. Security breach disclosure may also fall under the realm of policy compliance studies; however, the nature of public disclosure, which contains varying degrees of information content across several domains and involves a multitude of stakeholder influences, cannot be neatly categorized into a “compliant” or “non-compliant” dichotomy. There are multiple shades of grey and management discretion in terms of how organizations choose to voluntarily disclose the details of a negative event (Verrecchia, 1983; Dye, 1985; Skinner, 1994). Economic theories have shown that the issues of disclosure are more nuanced as there are multiple interested roles and affected stakeholder involved, and each may be motivated and incentivized by different factors and conditions that would lead to complexities in disclosure (Verrecchia, 2001). Regulators need to set up a minimum baseline requirement for disclosure; however, researchers have pointed out that specificities for disclosure regulations such as Healthcare Information Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX) are often ambiguous and difficult to define (Kulynych & Korn, 2003; Jain & Rezaee, 2006). On the other hand, from the organization’s perspective, there is a need to satisfy the regulatory requirements. However, security breach disclosure is a public-facing function, and the disclosure of negative events would invariably contain information content that would signal the quality of the organization to the general public, or lead to public scrutiny of its operations (Berezina et al., 2012). Therefore, there are motivations to withhold “bad news” altogether or strategically time the release of bad

news so as to preempt public reaction or to confound the signals with release of good news (Dye, 1985; Aboody & Kasznik, 2000; Kothari et al., 2009).

Although there has been research in various disciplines on policies, security management, compliance behavior, and mandatory or voluntary disclosure, there is no research to-date directly examining the issues of security breach disclosure. There is a lack of understanding and consensus on what breaches need to be disclosed and little evidence on how actual practices are employed by breached organizations. Overall, the field of information systems research as a whole has yet to develop a comprehensive framework which allows us to explore and understand the roles and conditions that lead to difference choices and actions in security breach disclosure. Despite its urgency and importance to society, recent phenomena have showed us that security breach disclosure remains a challenging and confusing subject for policy makers, practitioners, and researchers.

1.2.1 Current Challenges in Research

In recent years, a small number of empirical and theoretical researchers have started to investigate the issue of security breaches. Among their studies, investigation of the economic consequences of breaches on an organization's stock market price account for the majority of the work so far (Campbell et al., 2003; Cavusoglu et al., 2004; Acquisti et al., 2006; Kannan et al., 2007; Gordon et al., 2011). The line of research on security breach disclosure, although gaining interest, still faces several challenges. The challenges can be summarized as follows:

- **Data availability:** It is generally difficult to obtain detailed information on security breaches from affected organizations due to its sensitivity and possible negative impact of its publicity. Incomplete data, typically due to organizational propensity to withhold public disclosure of negative news, may result in misleading statistical inferences as the phenomenon drawn from the sample data may not adequately reflect the empirical reality.
- **Evidence gathering:** There are difficulties in extracting relevant evidence as reports may be intentionally ambiguous, or lack detail and transparency. Although there are many potential sources for security breach disclosures, the data are often unstructured and of varying quality. As indicated by Garg et al., (2003), although empirical research has attempted to quantify the magnitude of losses resulting from breaches in IT security, reliance on self-reported company data has resulted in widely varying estimates of limited credibility.
- **Cross-referencing and Interpretation:** There are often difficulties in obtaining deeper understanding that require the analysis of unobserved patterns from large numbers of textual documents. Breach data such as software or hardware logs are often difficult to interpret or to draw theoretical inferences from.

1.2.2 Current Challenges in Practice

The lack of awareness of information security policies is commonly recognized as one of the major threats to ISM (Information Security Management) (Bulgurcu et al., 2010). It is logical to infer that ambivalence, naivety, or lack of knowledge about the requirements for security breach disclosure could be the main challenges for effective disclosure.

More specifically, in terms of practice, the current challenges facing effective disclosures can be summarized as follows:

- Lack of clear standards, guidelines, or policies on what needs to be disclosed, when to disclose, and through what channels the disclosures should take place;
- The firm's intrinsic motivation to withhold information and to avoid public embarrassment;
- Penalties for non-disclosure and non-compliance are seldom explicit and are often non-existent.
- Lack of standards that could serve as benchmarks or measures of disclosure compliance do not exist.

1.2.3 Challenges for Policy Makers

Recognizing the importance of proper disclosure, government agencies and regulators throughout the world have started introducing new legal frameworks or are accelerating efforts at enforcing regulatory requirements. Regulations, the primary tool for policy makers, are intended to stimulate and enforce changes with respect to disclosure practices, so that stakeholders can be informed. New legal frameworks for disclosure generally have been built around the following principles: (Regan, 2009)

- *Stakeholder Information needs*: The public's need for adequate information;
- *Timeliness*: To provide the affected party timely information regarding the breach so that proper remediation efforts can be taken to prevent further damage.

- *Transparency*: The need for clear, unambiguous communications following a security breach;
- *Enforcement*: A greater prescription of legal obligations so that appropriate sanctions and penalties are better-known for those who fail to disclose

Security breach disclosure, at the minimum, satisfies regulatory requirements and provides important information to affected parties. Proper disclosures also provide essential input to the organization's ISM process and enhances the feedback loop that would assist stakeholders in learning from past security mistakes and prior incidents (West-Brown et al., 2003). For the information security community as a whole, security breach disclosures add to the knowledge-building process so that new knowledge is accumulated through experience. If the process is ineffective, it would result in inadequate controls to prevent future breaches. The current issues surrounding security breach disclosure are urgent and important. They warrant a systematic and comprehensive effort to carefully examine the current landscape of policy and practice, and provide a method to evaluate our current understandings so that meaningful advancements can be made. I intend to challenge these tasks through this research.

1.3 Research Questions

This research is an exploratory study on the issues and phenomenon of security breach disclosure. The main objective of this research study is to explore the disclosure requirements elements, current disclosure practices, quality measurements, and provide a substantive framework that maps out future research paths and topics in the study of

security breach disclosure. The overall goal is to provide a better understanding of the issues to society and to foster future research. To facilitate this goal, the research questions specified in this section act as a directional guide to aid the exploration and evaluation of policies and practices that together present a systematic view of cybersecurity breach disclosure.

Grand-tour research question:

What is the current landscape of security breach disclosure, its requirements, practices, role, factors, and conditions that affect security breach disclosure?

Security breach disclosure, defined in this study, is a process of reasoned actions, decisions, and controls that organizations exercise toward disclosing information surrounding a security breach. Through different stakeholder influences, internal and external factors, the process often leads to varying degrees of completeness, accuracy, timeliness, transparency, and management involvement in the information communicated to relevant stakeholders for decision making. The grand-tour research question grants us the opportunity to explore and understand the phenomenon and investigate relevant issues using a combination of qualitative and quantitative research methodologies.

Research question 1: (RQ1) –Breach disclosure requirements

What are the common elements of security breach disclosure requirements?

The study starts by exploring what are the domains and requirements of security breach disclosure. Existing regulatory requirements on security breach disclosure differ greatly from jurisdiction to jurisdiction. Some industries, such as healthcare and the financial sector, may also have different regulatory requirements. This research question is important as there is a vacuum of understanding of not only what *should* be required but also what *are* currently required by law. To explore the landscape of security breach disclosure, this first research question help establish the groundwork by reviewing current regulations from the EU, United States, and Canada concerning the practice of disclosure to identify the common domains of compliancy requirements.

Research question 2: (RQ2) – The information content

What information has been contained in security breach disclosures?

This research question explores the current practices of public disclosures. To extract knowledge from security breach disclosures, it is necessary to investigate the evidence from actual practices and examine the information content contained in the disclosure

reports. While research on information security topics has gained momentum in recent years; little research has focused on using evidence from actual breaches. This results in a lack of understanding in how organizations are reporting security breaches and what information content is actually covered in their reports. RQ2 examines current practices by extracting the information content from the common elements established in RQ1.

Research question 3: (RQ3) – Evaluating security disclosure

*How to measure the varying degrees of disclosure and
their relations to the elements of disclosure
requirements?*

This research question concerns with the need to investigate the quality of disclosure. A typical security breach disclosure may include information regarding descriptions of the threat sources, the nature of the events, the potential impacts, and potential resolution. At the minimum, the organization must have adequate security policies and sufficient controls to enable internal disclosure so that the security problems are communicated with transparency to senior management and to the Board (Grance et al., 2004, Cichonshi et al., 2012). At a higher degree, the organization may go above and beyond the minimum disclosures required by regulations and strive to voluntarily signal quality and responsibility of the organization towards their stakeholders (Polinsky & Shavell, 2010). RQ3 aims to establish measuring methodologies and instruments to benchmark organizational efforts towards the three domains of quality: completeness, time

references, and overall management involvement in the security breach disclosure process.

Research question 4: (RQ4) – Framework of security breach disclosure

What are the future research directions for security breach disclosure?

The final research question concerns future research in security breach disclosure. By using stakeholder analysis and considering the stakeholder roles that include both internal and external influences on the organization, this study proposes a framework that queries what are the dynamics between stakeholders on security breach disclosure policies, practices, and knowledge-building. In essence, RQ4 is concerned with mapping future research paths and directions through the framework that illuminates the roles and interactions between the stakeholders -- what are their roles in setting the requirements, in composing the disclosure, in evaluating the effort, and in learning and accumulating knowledge for the community as a whole.

1.4 Research Objective

The main objective of this study is to understand the phenomenon of security breach disclosure through existing policies, practices, and stakeholder interactions. The ultimate goal is to strengthen our understanding of security breach disclosure and enhance the accumulation and transfer of knowledge obtained through security breach disclosure;

thereby providing organizations, regulators, and the information security community with the information necessary to develop policies, tools, and controls for identifying, managing, and reducing the risks of future breaches. Guided by the goal, this study sets the following four main objectives:

1. To understand disclosure requirements:

The first objective of this study is to understand the landscape of security breach disclosure requirements. This is accomplished by reviewing current disclosures and querying current evidence of practice. This research question is important as the lack of understanding of requirements leads to problems in practice and enforcement. The output is intended to establish a set of common elements and structure in disclosure reports that would enhance practice and enable future research inquiries through a structured taxonomy of information content. In addition to setting up the groundwork for subsequent research questions within this study, these common elements could potentially inform future practices and policies, strengthening the information content of future disclosures.

2. To understand current disclosure practices

The second objective purport to understand and examine current disclosure practices. This is accomplished in two phases. First, I review various breach disclosure practices currently employed by the practitioners; this enables us to understand different types of security disclosures and their respective purposes and audiences. In addition to

reviewing current practices, the second phase aims to build on RQ1 and examine the current practices in public notification / customer notification. RQ2 leads the investigation into the information content of public breach disclosure. The objective is to understand what has been disclosed to the public by organizations subsequent to a security breach. In terms of methodology, the novel use of combining GTM (Grounded Theory Methodology) and computerized textual analysis allows future research to extract information content from unstructured documents to structured data for analysis. Although this goal is not expressly emphasized, the potential contribution to the academic community is nonetheless important for future research.

3. To evaluate disclosures

Third, this study aims to develop new measures and instruments to evaluate the quality of public disclosure. This is an important issue as the lack of benchmark and measuring tools has led to difficulties in enforcing adequate disclosure. The output would include replicable methods to evaluate disclosure so that each report is benchmarked using a consistent instrument that would assist policy makers and the information security community in evaluating the compliance effort and the quality of the disclosure.

4. To expand future research on security breach disclosures.

Fourth, this study aims to explain the roles and interactions of stakeholders affecting the efficacy of the disclosure practices. Output of the fourth objective includes a theoretical framework of security breach disclosure which would assist future researchers in finding

research topics and position new studies in the larger picture. This research question is important as we are still in the early stage of breach disclosure study. The area is young and there still exists many potential question not yet explored. The framework will encourage scholars to find new avenues in the area, develop more in-depth research questions, and provide more nuanced examination of the phenomenon.

1.5 Research Approach

1.5.1 RQ1 - The Common Elements of Security Breach Disclosure

To answer RQ1, this research surveys recent breach disclosure regulations from the EU, United States, and Canada against evidence of disclosure to conclude the domains of compliancy requirements. The use of GTM in this stage allows the identification of the core phenomenon of breach disclosure and develops the common elements that tie together the roles, context, conditions, actions, interactions, and consequences that characterize the dynamics of the security breach disclosure process.

1.5.2 RQ2 - Extracting Disclosure Information Content

This study employs a novel approach that combines the strength of human processing (GTM) and computerized textual analysis to accomplish the task of information extraction. From the common elements developed in RQ1, this study constructs specialized lexicon and extraction rules using common elements defined through GTM; then textual analysis techniques are employed to extract evidence of compliance programmatically. This approach ensures the development of a theory based on the sensitivity of the human process, while incorporating the efficiency and reliability

features of computerized textual analysis. After extraction, the information contents are compiled into an accompanying XML document that are used in RQ3 for further analysis.

1.5.3 RQ3 - Evaluating Security Disclosure

The objective of RQ3 is to determine the quality of disclosure report and degree of effort from the breached organization. To accomplish this objective, this study surveys quality measures from the accounting literature, which has a well-established line of research on developing matrices and measuring instruments for disclosure. Using the common elements defined in RQ1 and the information content extracted from RQ2, I develop three measures that serve as quality proxies – the completeness of report coverage, the time references of relevant events that occurred, and management involvement in the incident response process. Following prior studies (Botosan, 1997; Botosan & Plumlee 20024), the evaluation stage uses a points system to calculate the rating score. In the final stage of RQ3, I employ a generalized least squares model and logit regression model to find factors that contribute towards quality.

1.5.4 RQ4 - Future of Security Breach Disclosure

RQ 4 asks the salient question “what are the future research directions for security breach disclosure?” To investigate this question, a “map” is needed in aiding the exploration of future research paths and directions using a framework that would lay out the inter-relationships and stakeholder roles in security breach disclosure. The approach considers the role and relationships of four main stakeholders: the regulators, management of the breached organization, the affected parties, and the information

security community. From this framework, the paths and areas that warrant research are quickly illuminated as the researcher plans future studies in a systematic manner, developing research programs that would contribute toward the accumulation of knowledge in the field of security breach disclosure.

1.6 Summary

This study is completed at a crucial turning point of security breach disclosure. Recent cases such as the breaches at Equifax, Yahoo, Uber, and even Facebook have attracted attention from the public and put significant pressure on regulators. However, the lack of understanding has hampered our ability in defining the requirements, enforcing practice, evaluating the disclosure content, and improving future policies and practice. These issues warrant considerable effort to examine the current landscape of policy and practice and provide a method to evaluate current understanding so that meaningful advancements can be made.

This is an ambitious inter-disciplinary study to derive an evidence-based understanding of security breach disclosure. The tasks include surveying current theories, literature, regulations, practices, establishing quality matrices, and mapping future research paths and directions through a framework. The grand-tour research questions guide the study through four main research questions. The following Table 1-1 summarizes the research question, focus, objective, approach, and output of this research.

Table 1-1 Summary of Research Question, Focus, Objective, Approach, and Output

Research Questions	Focus	Objective	Approach	Output
What are the common elements of security breach disclosure requirements?	Current disclosure laws and regulations	To understand disclosure requirements	Qualitative approach - review of current disclosure regulations and examine evidence of current practice	Common elements of security breach disclosure
What information has been contained in security breach disclosure?	The information content of public disclosure	To understand the information content of current practices in public disclosure	Qualitative approach - Using a combination of GTM and textual analysis to extract and communicate the knowledge obtained from breach disclosure	Evidence of current disclosure practices in terms of the common elements
How to measure the varying degrees of disclosure and their relations to the elements of disclosure requirements?	The quality matrices and measuring instruments of disclosure	To evaluate and benchmark disclosure	Quantitative approach - Using information extracted to evaluate the degree of completeness, time references, and management involvement in disclosure	Quality matrices and measurement tools in terms of disclosure completeness, time references, and management involvement.
What are the future research directions on security breach disclosure?	Future of disclosure regulations, practices, and research	To establish a framework that maps future research directions and paths	Qualitative approach - analyze stakeholder interactions through proposed framework of security breach disclosure	Security breach disclosure framework and future research directions

The remaining chapters are organized as follows: Chapter 2 discusses the essential facets of security breach and disclosure through a review of definition, current state of research, practices, and policies. Chapter 3 reviews economic theories and the conceptual background on mandatory disclosure, voluntary disclosure, and management discretion in the control of disclosure. Chapter 4 starts the investigation of research question 1, focusing on the current disclosure regulations adopted by various US, EU, and Canadian government agencies with the objective of establishing a set of common elements of disclosure. In Chapter 5, the common elements concluded from RQ1 are used to extract the information content of current security breach disclosures in a structured, systematic manner. Using a sample of 859 actual disclosures, obtained from the California Attorney General's Office covering the period from 2012 to 2016, Chapter 5 focuses on the information content of breach disclosure with the objective of obtaining better understanding of current public disclosure practices in terms of what are actually disclosed. Chapter 6 investigates RQ3 which focuses on the evaluation of disclosure reports. The objective is to determine the quality and degree of effort from the breached organization. The development of the measuring instruments and evaluation matrices are explained in detail. Chapter 7 focuses on the future of disclosure regulations, practices, and research with the objective of exploring future research paths and directions through the proposed security breach framework. Chapter 8 concludes the study with summaries of findings, research significance, and recommendations towards better disclosure practices.

2 The Essential Facets of Security Breach & Breach Disclosure

2.1 From Security Incident to External Breach Disclosure

Security incidents, security events, data breach, or even “a hack” have been used interchangeably with overlapping meanings to describe the phenomenon when an adverse event has occurred that leads to unauthorized access to system, loss of data, or loss of processing capability. According to the National Institute of Standards and Technology (NIST), a *security incident* is defined as “*a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.*” (NIST SP800-61, 2012)

Under this definition, examples of incidents could include: (Cichonski et al., 2012)

- Denial-of-Service attack: An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Ransomware attack: The attacker uses encryption or other means to restrict user access to data, with the purpose of demanding ransom payment.
- Phishing attack: Users are tricked into performing actions or running tools that would allow attacker access to confidential data or restricted system resources.
- Blackmail and espionage attack: An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.

- Internal data theft: An internal user provides or exposes sensitive information to others through theft or peer-to-peer file sharing services.

The above examples are not exhaustive; there are many different types of security incidents that an organization might encounter. Not all security incidents would lead to breach of confidential data, and by the same token, not all breaches of confidential data would necessary lead to breach of consumer personal identifiable data (PID). Actual breaches could take many forms and have different implications to the organization. For example, Campbell et al. (2003) found a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach does not involve confidential information. Small-scale security incidents may be directed at disrupting specific business functions, such as denial of service attacks on web servers, databases, or network appliances (Cichonski et al., 2012); while large-scale security incidents may target companies that operate in industries responsible for critical infrastructure. The attack may be targeted by organized cybercriminal syndicates using sophisticated tools and offered as a “service” (Barber, 2001; Manky, 2013; FBI, 2017); while some attacks may result from “script-kiddies” that run easily obtainable toolkits freely available on the Internet (Meyers et al., 2009).

NIST’s definition of security incident allows a broad generalization of various adverse events with potential negative consequences. However, NIST’s objective is to highlight the need for incident response as there could be an infinite number of different causes that would require the organization’s attention when an incident occurs. For the purpose

of security breach disclosure, depending on the regulators' objective, the definition may focus on a specific type of security incident. For example, The California regulation defines *security breach* as “*unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business*” (California Civil Code, 2000, Section 1798.82). In this example, the definition focuses on “*unauthorized acquisition of computerized data*” which may neglect other types of security incidents where no computerized data were involved. To demarcate the differences between common security incidents and security breaches, there are also proponents of using a more clear definition separating the two (Verizon, 2017), specifying *security incident* as “*a security event that compromises the integrity, confidentiality or availability of an information asset;*” and, defining *security breach* as “*An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.*”

Although there is some accord among industry participants on the definition of “security incident” and “security breach”, there is no general consensus on the definition and conditions that warrant public disclosure. The lack of a clear definition on the conditions creates additional complexities in security breach disclosure in terms of enforcing regulatory requirements and identifying what type of security incidents would warrant a particular type of disclosure. Is a public disclosure necessary if a security incident involves no loss to customer *privacy* data? For example, would a theft of *private* data, such as an organization's trade secret, warrant disclosure? On the other hand, would an intentional abuse of privacy data and systemic breach of user policies, such as foreign

agent use of a Facebook social network to interfere with a public election, warrant disclosure?

The discussion of security breach disclosure must therefore start with the classification security breach and identify the conditions that warrant public notification or disclosure. Common sense would suggest that a security breach that involves no data breach on customer data would not require a public disclosure. Indeed, this is used by the majority of US State level disclosure regulations (Sullivan & Maniff, 2016); however, loss of privacy or theft of personal data is not the *only* concern to the public. A security breach to critical infrastructure services such as energy and water, even without any data loss, could have important implications to public safety. In these cases a public disclosure would be warranted (Lewis, 2014; Knapp & Kangill, 2014). More recently, the breach of user policy of Facebook by Cambridge Analytica (The Guardian, 2018) and foreign agents (Bloomberg, 2018) further challenges our current definition and conditions of security breach disclosure.

It is not in the interest of this study to suggest a rigid definition and disclosure condition that would encompass all security breaches for all types of organizations. Rather, it is important to raise the awareness that the definition and classifications of security breach, as well as the conditions for disclosure, must be clarified by the regulator or by the organization to the extent that the responsibility of internal or external disclosure could be associated with the functional area within the organization. This study adheres to the NIST Computer Security Incident Handling Guide (NIST SP800-61, 2012), that "*one of*

the first considerations should be to create an organization specific definition of the term ‘incident’ so that the scope of the term is clear.” The reason why an organization-specific definition or classification is necessary is due to the fact that when an incident occurs, it would inevitably raise security implications that are unique to the organization’s operation and their involvement in public safety and security concerns (for example, GPS location data in popular photo-sharing services). Therefore, organizations need to define their own specific conditions to activate and mobilize certain functions and processes within the organization to handle the incident and disclosure effort. The definition and conditions for disclosure could be adopted from an industry-wide commonly agreed practice based on different classifications of security events. However, the responsibilities and disclosure practices should be specific to the organization because, without a clear delineation, the incident handling processes would fall into confusion and disarray.

The following diagram (Figure 2-1) shows graphically that publicly disclosed security breaches constitute only a small fraction of security incidents that organizations experience. It also highlights the need of clear delineation for responsibilities in the disclosure process. From the diagram, a security incident might not be publicly disclosed, if the following conditions are not satisfied:

- must be discovered by the detection control or external sources;
- must be reported internally upward to the management and downward to the personnel in charge of incident response;

- must satisfy the conditions that warrant external disclosure; this is due to the fact that not all security incidents result in the breach of personal data or “foreseeable harm” to the affected party;
- must be free from management discretion or intentional interference in publicly disclosing the breach and the information surrounding the breach.

If any of the above four necessary conditions are not satisfied, or the responsibilities are not cleared stated, a security incident would likely “fall through the cracks” and not be publicly disclosed. In the case of management interference, it could potentially come in the form of manipulating the internal reporting process to avoid internal disclosure, or to manipulate the impact assessment that would alter the impact so that it would not satisfy the condition for external disclosure, or in some cases such as UBER, avoid disclosure despite the fact that all the conditions were met.

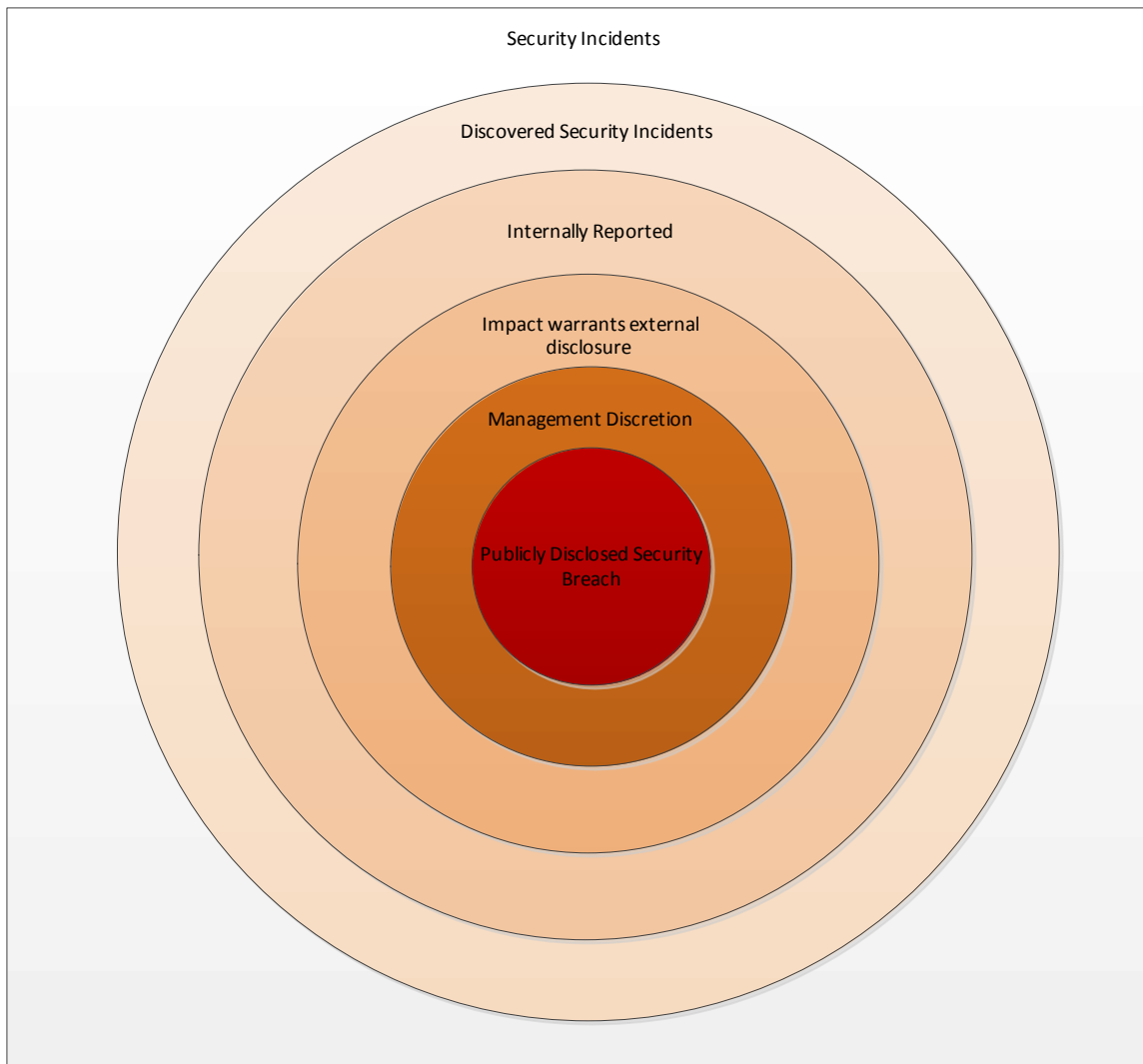


Figure 2-1: From Security Incidents to Publicly Disclosed Security Breach.

2.2 Review of Current State of Research

2.2.1 Economic Consequences of Disclosure

Many researchers have studied the effects of breach disclosure on stock market outcomes.

For instance, Campbell et al. (2003) investigated the economic cost of publicly announced information security breaches and found the nature of the breach affects a

firm's stock prices. In particular, they found significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach did not involve confidential information. Thus, stock market participants appear to discriminate across types of breaches when assessing their economic impact on affected firms. Cavusoglu, Mishra, and Raghunathan (2004) found that the public disclosure of a security breach results in the loss of, on average, 2.1 percent of their market value within two days of the announcement, that is an average loss in market capitalization of \$1.65 billion per breach. Telang and Wattal (2007) find that software vendor stock prices suffer when information about their products' vulnerability is announced. Acquisti, Friedman, and Telang (2006) used an event study to investigate the impact on stock market prices for firms that incur a privacy breach and found a negative and significant, but short-lived, reduction of 0.6 percent on the day when the breach is disclosed. Interestingly, Ko and Dorantes (2006) studied the four financial quarters following a security breach and found that, although breached firms' overall performances were lower relative to firms that incurred no breach, their end of year sales increased significantly relative to firms that incurred no breach.

This stream of studies shows that security breach disclosure provides a credible signal to investors, whose response can be observed through stock price reactions to the public security breach disclosure. However, research is less conclusive regarding the information content of disclosure, namely, what are actually disclosed. Without an understanding of the information content of the breach, the stock market reaction, arguably, might be just a generic reaction to bad news. Ko and Dorantes's (2006) finding

that breached firms' overall financial performance “bounced back” in end of year sales support this assumption. In addition to lack of understanding of the information content in security breach, no study has been done to investigate management's effort towards compliance or violation towards disclosure and provide methods and measuring instruments to evaluate their effort and the quality of disclosure. In other words, current research is oblivious regarding how public security breach disclosures are conducted.

Research on breach notification practices and policies is at an early stage but has nevertheless shed some light on the mechanisms and effects of disclosure. For example, Romanosky et al. (2011) showed that notification laws can reduce the rate of identity theft, and suggest that oversight and enforcement might be needed to encourage compliance. In terms of effect on affected parties, they hypothesize that after disclosure requirements are implemented, more consumers will be notified of breaches and in turn will take steps to protect themselves, thereby reducing the incidence rate of future identity thefts. Their results show that adopting a notification law reduced identity theft by an estimated average of 6.1 percent, resulting in a mean reduction in the cost of identity theft of \$93 million in United States.

However, certain aspects of notification laws can strongly influence their effectiveness. Organizations that suffer a breach have incentives not to notify customers, in order to avoid the costs and consequences of disclosure. Laube & Bohme (2017) investigate this incentive in a theoretical model and show that including a periodic audit requirement for security systems can greatly enhance the effectiveness of notification laws.

The language used to notify consumers may also influence the effectiveness of these regulations. Breach notification laws provide organizations some level of management discretion in how they inform customers about a breach, which can lead to suboptimal outcomes for affected consumers. Bisogni (2015) studied a sample of notification letters sent in 2014 to consumers whose data were exposed and found that, while these letters complied with notification laws, some organizations sending them understated the seriousness of the breach to reduce their reputational damage.

Furthermore, a notification law's efficacy can depend on how quickly it requires organizations to disclose information in the event of a breach. Bisogni (2015) showed that consumers were at risk for a considerable time prior to notification: the average time between an organization discovering a breach and notifying consumers was 35 days. More troubling, the average time between when a breach actually occurred and notification was 117 days. In other words, organizations are often unaware of the breach for an extended period in which potential harm could occur.

Overall, the field of information systems research has illuminated the effect of security breaches and the effect of implementation disclosure requirements. However, the field as a whole has yet to develop a reasonable understanding on what are required, what are reported, and how to evaluate disclosure reports. It also remains unclear with respect to what are the reporting specifics that need to be established that would lead to better disclosure practice; and what factors and incentives would motivate organizations

towards better disclosure above and beyond the minimum mandatory disclosure requirements.

2.2.2 Other related literature on disclosures

Prior literature, particularly in the accounting and finance stream of research, has given ample evidence which indicates that timeliness and reliability are crucial elements for information disclosure as the two properties of decision-relevant information that are critical factors in determining the usefulness of financial information (Givoly & Palmon, 1982). Timeliness can be measured relatively easily as a quantitative measure and is also an important qualitative attribute meaning that the disclosed information should reach the interested parties as soon as possible (Carslaw and Kaplan, 1991). On the other hand, reliability, although an attribute promoted by IASB (2005), is not defined clearly.

2.2.3 Timeliness and Disclosure Delay

Studies in the accounting and finance stream literature also shows that firms tend to delay disclosure if there are indications that the information content of the report could be negative for the market (Chamber and Penman, 1984). Kasznik and Lev (1995) reports that companies preparing to inform about bad news tend to give more discretionary disclosures than the companies with good news. Kasznik and Lev (1995) suggests that the larger the “surprise”, the bigger the probability of management discretion in disclosures. Lee et al. (2008) suggest that the length of the discretionary reporting lag could depend on manager opinion on optimal timing while taking into account the costs and benefits arising from it. These studies provide some peripheral evidence that could

be used to explain security breach disclosure delay; however, no research has studied security breach disclosure delay directly.

2.2.4 Quality of disclosure

Studies that discuss the quality of disclosure are quite established in financial accounting literature but very little research on this topic could be found in IS (Information Systems) research. This may be due to the fact that there are much fewer IS related mandatory disclosure requirements and governing agencies than there are financial accounting related disclosures. In financial accounting terms, disclosure quality stems from the *“overall quality of financial statements and it refers to the extent to which the published information describes the financial position and operations of the company”* (Robinson and Munter, 2004). The International Accounting Standards Board’s (IASB) conceptual framework defines two qualitative characteristics: relevance and reliability. IASB’s conceptual framework states that the disclosure is relevant if it influences the economic decisions of users. According to Bowrin (2008), relevance is strictly related to the information’s ability to affect user decision making and timeliness is one part of relevance. Further, reliability means the extent to which the disclosures are free from material errors (Bowrin, 2008).

Although the definition of quality can be described quite easily in the broader context, many researchers argue that the description of quality is relatively complex and a wide consensus among academics does not really exist on its definition (Botosan, 2012). However, the quality of disclosure should have at least the characteristics that make the

information contained in the disclosure “valuable” to the information receiver in terms of assisting the relevant stakeholders making decisions after a security breach. For that reason it is rational to examine aspects of the information content, such as relevancy, timeliness, or management involvement that would affect the quality of disclosure.

Overall, the need for understanding security breaches is well-recognized and the topic has drawn considerable attention from academic researchers and industry practitioners. On the other hand, the literature on disclosure spans several disciplines and various schools of management. However, from the IS perspective, due to differences in the paradigm, core assumptions, and methodologies, the study of security breach disclosure has not yet flourished, and current studies do not provide an in-depth understanding able to inform policy and practice.

2.3 Review of Current Practices of Breach Disclosure

2.3.1 Internal Disclosure

Disclosure is an essential part of an organization’s overall incident response management process that encompasses not only external but internal disclosure and reporting processes. So when a security incident occurs, members of the organization can follow defined procedures to collect, verify, record, and report the incident (West-Brown et al, 2003). When setting up internal disclosure and reporting guidelines, management needs to be aware that non-malicious security violations (Guo et al., 2011) or accidental errors could very likely motivate employees to conceal the incident and avoid reporting the incident. On a higher level, the Board or people who are responsible for governance also

need to be aware that management may avoid internal disclosure if they perceive a potential negative consequence to their performance review and incentive contracts (Baker et al., 1994; Bergstresser & Philippon, 2006). A recent survey (ALM Intelligence, 2017) found that nearly 40 percent of U.S. organizations fail to disclose security issues to their board. In addition, the survey found that only 14% of the incident response management plans include draft communications documents; and only 5% include draft notices to regulators.

2.3.2 Initial Notification

Subsequent to a security breach incident, the organization could take various measures to notify external parties of the security incidents. These external parties could include governing agencies, business partners, vendors or customers, third party auditors, and the general public. Depending on jurisdiction, some regulators require an “immediate” initial notification to the regulator even though facts about the breach might not be fully available. For example, the new General Data Protection Regulation (GDPR) in EU, implemented on May 25, 2018, states that an initial notification must be made to the regulator within 72 hours after becoming aware that a personal data breach has occurred; even if the full details are not available.

Initial notification is usually followed up with a second notification to provide further information. The justification of the deadline is debated (McQueen et al., 2011). While the timeliness of reporting could be important, without adequate details the initial disclosure could lead to panic, confusion, or even “security fatigue” (Furnell & Thomson,

2009). The tradeoff between timeliness and reliability of the disclosure is an area that attracts quality research in the financial accounting stream of literature (Gigler & Hemmer, 2001; Healy & Palepu, 2001). In the IS literature, Ballou et al. (1995) explored the balance between accuracy and timeliness in the setting of designing information systems that would optimize the tradeoff. In terms of security breach disclosure, the argument for the tradeoff is that the assessment of the breach will improve with the passage of time. The same situation exists for many processes such as investigation, impact analysis, and remediation. However, as a consequence of the dynamic nature of security breaches, the information also becomes less relevant over time. Although initial notification is being considered in many other jurisdictions other than the EU, there is considerable pushback from practitioners (Porter et al., 2018).

2.3.3 Customer/individual Notification

As security breach laws around the world continue to evolve, regulations on data breach notification requirements for customers and affected individuals are becoming more stringent (Shey et al., 2017). When a security breach involves the loss of individual data such as personal identifiable information of customers or private patient data, an external-facing disclosure to the affected party is usually required by regulators. The external-facing customer communication following a breach is a critical component of incident response. It is the first step in reassuring consumers that organization is handling the security incident adequately (West-Brown et al., 2003). The manner of the communication sets the stage and sends out a strong signal about the organization's capability in handling negative events and retaining the trust of their customers (Hearit,

2006). Figure 2-2 shows a typical customer notification report, which contains a description of the breach, potential impacts, and remediation solutions.

Notifying affected individuals could be facilitated in many different forms. Most regulations require a “written notification” such as a notification letter or email to the affected individual with contact information if further information is desired to address the individual’s particular concerns. However, as many security breaches are technical in nature, the receiver of the notification may not be able to understand the nature or the significance of the event. To address this potential knowledge gap and avoid confusion, regulators such as California Attorney’s General Office require security breach notification *“shall be written in plain language, shall be titled ‘Notice of Data Breach,’ and shall present the information under the following headings: ‘What Happened,’ ‘What Information Was Involved,’ ‘What We Are Doing,’ ‘What You Can Do,’ and ‘For More Information.’”*

A particular issue regarding individual notification and overlapping regulations on security breach disclosure is the threat of “Security breach fatigue” (Ablon et. al, 2016). The fundamental purpose of individual breach disclosures is to help the affected individuals understand the issue so that adequate steps can be taken to prevent further damage. However, others (Edwards & Forrest, 2016; Chen, 2018) have pointed out that frequent news on security breach could have contributed to the phenomenon of security breach fatigue, where customers may receive multiple disclosures on one event, or ignore the disclosure altogether. It is also possible that the organization’s intention to avoid

public embarrassment by downplaying the significance and the potential impact could potentially contribute to the fatigue phenomenon; however, empirical evidence would be needed to further substantiate this claim.



Processing Center
P.O. Box 3825
Suwanee, GA 30024

John Q. Sample
123 Fake St.
Apt. 99
Austin, TX 77022

February 7, 2014

AllClear ID Redemption Code: [REDEMPTION_CODE]

Dear John Q. Sample,

Please read this letter carefully. As part of an ongoing investigation, we have been informed that three HR associates have been arrested on allegations that include the unlawful use of personal information belonging to current and former associates and a small number of candidates. These HR associates were employed by The Home Depot in positions of trust and therefore had authorized access to your personal information to perform assigned job duties. Out of an abundance of caution, we are notifying you of the possible unlawful use of your personal information. Our investigation indicates that your information may have been accessed by one of these three associates for unlawful purposes. The information that could have been accessed by the arrested associates includes your name, contact information, social security number, driver's license number, and any financial account numbers you may have provided us, and the longest period of employment for any of the three arrested associates goes back to February 7, 2011. Because we take this matter very seriously, we are conducting a thorough internal investigation, and we are working closely with appropriate government authorities.

Although we have found no evidence that your information was inappropriately used at this time, we want to make sure you can take appropriate steps to help prevent the misuse of your personal information. We have arranged for you to receive 12 months of identity protection from AllClear ID at no cost to you. AllClear ID offers Credit Monitoring that delivers secure, actionable Alerts to you by phone. This service also includes a \$1,000,000 Identity Theft Insurance Policy, the AllClear ID Investigations Team to assist you in the event that your information is used fraudulently, and AllClear ID Resolution Services, if needed, to assist you in restoring your credit file.

You may sign up online at enroll.allclearid.com or by phone by calling 1-877-263-7996. To sign up online, go to enroll.allclearid.com. You will need to provide the redemption code that is listed at the top of this page. Once you have entered your redemption code, click on "Sign up now" on the right side of the page and follow the website's instructions. Please note, part of the sign-up process may include receiving a phone call from AllClear ID soon after you initiate the registration process. You have 90 days from the receipt of this letter to register. The AllClear ID service will be valid for one year from the date you register.

The AllClear ID service may be helpful because one possible misuse of your information would be to open credit card or consumer loan accounts in your name without your permission. This is called "identity theft." The theft of your identity can lead to the loss of your credit worthiness and can cause collection agencies to try to collect debts from you that you did not create. To see if someone is misusing your information you can check your credit reports and your banking and other account statements to make sure that all of the accounts and transactions on those reports were made by you.

We encourage you to remain vigilant, and to regularly review and monitor relevant account statements and credit reports. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to your identity to local law enforcement, your State Attorney General's office, or the Federal Trade Commission. Information on how to make some of these reports is included in the Reference Guide that is part of this notice to you. You should also report the unauthorized accounts or transactions to the credit reporting agency from which you obtained the report.

You are entitled to one free credit report annually from each of the three national credit bureaus. To order your free credit reports, please read the Reference Guide. It includes contact information for each of the three major credit agencies. You also have the right to place a fraud alert or security freeze on your credit file to prohibit temporarily the opening of new credit accounts in your name. The Reference Guide below explains how to take these steps. You can also learn more about how to protect yourself from becoming a victim of identity theft by contacting the Federal Trade Commission www.ftc.gov/idtheft/ (full contact information is in the Reference Guide below).

The Home Depot | 2455 Paces Ferry Road | Atlanta, GA 30339

Figure 2-2: Example of a Customer Notification from Home Depot (Page 1/3)

2.3.4 Periodic Disclosure

Publicly traded firms are required to file periodic reports to disclose specified information on a regular and ongoing basis. These periodic reports include annual reports which require companies to make disclosures regarding their business and operations, risk factors, legal proceedings, management's discussion and analysis of financial condition and results of operations ("MD&A"), financial statements, disclosure controls and procedures, and corporate governance.

In October of 2011, SEC recommended including disclosures relating to cyber risks and incidents. Although not mandatory, firms are encouraged to voluntarily include additional security disclosures in the form of risk factors discussion in the annual report. In response to "increasing significance of cyber security incidents", SEC determined it is necessary to provide companies with further guidance on managing security risks and disclosures of such risks. On February 21, 2018, the SEC voted unanimously to approve the final rules on security breach disclosure that expands upon the previous guidance provided in October of 2011. The updated guidance emphasizes the criticality of establishing and maintaining comprehensive policies and procedures related to security risks and incidents. Companies are required to "*establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity.*" (SEC, 2018)

According to the SEC's final version of the guidance, companies should weigh the potential materiality of any identified risks and in the case of cyber incidents, the importance of any compromised information and the impact of the incident on the company's operations.


Periodic disclosure serves an important purpose by informing investors of underlying economic conditions of the firm; however, the nature of periodic disclosure only summarizes events that happened during a given period of time and is only provided at specific time intervals such as the firm's quarterly earnings announcements and year-end annual reports. In addition, the intended audiences for the disclosure are aimed towards the stock holder and financial statement users of the firm, not the affected parties of any security breaches.


2.3.5 Vulnerability Disclosure

Vulnerability disclosure is a particular type of disclosure in the information security industry. It is the practice of disclosing software or system vulnerabilities to vendors so that vendors could use the information and address the vulnerability in the form of a patch or system update (Cavusoglu et al., 2005). Vulnerability is an inevitable, inherent risk of information systems. Regardless of how much time and effort is placed into identifying and removing flaws in the development process, it is inevitable that defects or "bugs" will be discovered in information technology products. Vulnerability disclosures are typically made by third party researchers or "white hat" hackers. The information is essential to the installation of security patches from the vendors, anti-virus software,

vulnerability scanning tools, and intrusion detection systems. In the United States, the United States Computer Emergency Readiness Team (US-CERT) coordinates and collects such disclosures and notifies the vendors to issue patches or updates. Figure 2-3 presents an example of vulnerability disclosures collected by CERT, which includes information such as the applicable platform, likelihood of occurrence, demonstrative example of exploits, and potential mitigation.

Unpatched security vulnerabilities in systems are the primary reasons for security breaches; an important challenge from the knowledge management perspective is to determine how to manage the disclosure of knowledge about these vulnerabilities (Cavusoglu et al., 2007). This is because an unpatched vulnerability can be a serious problem as the computer software and hardware industry are dominated by a few large vendors such as Microsoft, Apple, CISCO, and Oracle to name a few. For example, an unpatched vulnerability in a widely-used operating system such as Windows XP could have serious consequences as it could affect millions of users.


Common Weakness Enumeration
A Community-Developed List of Software Weakness Types



[Home](#) > [CWE List](#) > [CWE- Individual Dictionary Definition \(3.0\)](#)

ID Lookup:

[Home](#) | [About](#) | [CWE List](#) | [Scoring](#) | [Community](#) | [News](#) | [Search](#)

CWE-287: Improper Authentication

Weakness ID: 287
Abstraction: Class
Structure: Simple

Status: Draft

Presentation Filter:

Description
When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct.

Relationships
The table(s) below shows the weaknesses and high level categories that are related to this weakness. These relationships are defined as ChildOf, ParentOf, MemberOf and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as PeerOf and CanAlsoBe are defined to show similar weaknesses that the user may want to explore.

- Relevant to the view "Research Concepts" (CWE-1000)
- Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (CWE-1003)
- Relevant to the view "Architectural Concepts" (CWE-1008)
- Relevant to the view "Development Concepts" (CWE-699)

Modes Of Introduction
The different Modes of Introduction provide information about how and when this weakness may be introduced. The Phase identifies a point in the software life cycle at which introduction may occur, while the Note provides a typical scenario related to introduction during the given phase.

Phase	Note
Architecture and Design	
Implementation	REALIZATION: This weakness is caused during implementation of an architectural security tactic.

Applicable Platforms
The listings below show possible areas for which the given weakness could appear. These may be for specific named Languages, Operating Systems, Architectures, Paradigms, Technologies, or a class of such platforms. The platform is listed along with how frequently the given weakness appears for that instance.

Languages

Class	Prevalence
Language-Independent	(Undetermined Prevalence)

Common Consequences
The table below specifies different individual consequences associated with the weakness. The Scope identifies the application security area that is violated, while the Impact describes the negative technical impact that arises if an adversary succeeds in exploiting this weakness. The Likelihood provides information about how likely the specific consequence is expected to be seen relative to the other consequences in the list. For example, there may be high likelihood that a weakness will be exploited to achieve a certain impact, but a low likelihood that it will be exploited to achieve a different impact.

Scope	Impact	Likelihood
Integrity	Technical Impact: Read Application Data; Gain Privileges or Assume Identity; Execute Unauthorized Code or Commands	
Confidentiality		
Availability	This weakness can lead to the exposure of resources or functionality to unintended actors, possibly	
Access Control	providing attackers with sensitive information or even execute arbitrary code.	

Likelihood Of Exploit
High

Demonstrative Examples
Example 1
The following code intends to ensure that the user is already logged in. If not, the code performs authentication with the user-provided username and password. If successful, it sets the loggedin and user cookies to "remember" that the user has already logged in. Finally, the code performs administrator tasks if the logged-in user has the "Administrator" username, as recorded in the user cookie.

Example Language: Perl (bad code)

```

my $q = new CGI;

if ($q->cookie('loggedin') ne "true") {
    if (!AuthenticateUser($q->param('username'), $q->param('password'))) {
        ExitError("Error: you need to log in first");
    }
} else {
    # Set loggedin and user cookies.
    $q->cookie(
        -name => 'loggedin',
        -value => 'true'
    );

    $q->cookie(
        -name => 'user',
        -value => $q->param('username')
    );
}

}

if ($q->cookie('user') eq "Administrator") {
    DoAdministratorTasks();
}

```

Unfortunately, this code can be bypassed. The attacker can set the cookies independently so that the code does not check the username and password. The attacker could do this with an HTTP request containing headers such as:

```
(attack code)
GET /cgi-bin/vulnerable.cgi HTTP/1.1
Cookie: user=Administrator
Cookie: loggedin=true

[body of request]
```

By setting the loggedin cookie to "true", the attacker bypasses the entire authentication check. By using the "Administrator" value in the user cookie, the attacker also gains privileges to administer the software.

Example 2

In January 2009, an attacker was able to gain administrator access to a Twitter server because the server did not restrict the number of login attempts. The attacker targeted a member of Twitter's support team and was able to successfully guess the member's password using a brute force with a large number of common words. Once the attacker gained access as the member of the support staff, he used the administrator panel to gain access to 33 accounts that belonged to celebrities and politicians. Ultimately, fake Twitter messages were sent that appeared to come from the compromised accounts.

Example 2 References:

[REF-236] Kim Zetter. "Weak Password Brings 'Happiness' to Twitter Hacker". 2009-01-09.
<<http://www.wired.com/threatlevel/2009/01/professed-twit/>>.

▼ Potential Mitigations

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use an authentication framework or library such as the OWASP ESAPI Authentication feature.

▼ Memberships

This MemberOf Relationships table shows additional CWE Categories and Views that reference this weakness as a member. This information is often useful in understanding where a weakness fits within the context of external information sources.

Nature	Type	ID	Name
MemberOf	V	635	Weaknesses Originally Used by NVD from 2008 to 2016
MemberOf	C	718	OWASP Top Ten 2007 Category A7 - Broken Authentication and Session Management
MemberOf	C	724	OWASP Top Ten 2004 Category A3 - Broken Authentication and Session Management
MemberOf	C	812	OWASP Top Ten 2010 Category A3 - Broken Authentication and Session Management
MemberOf	C	930	OWASP Top Ten 2013 Category A2 - Broken Authentication and Session Management
MemberOf	C	935	OWASP Top Ten 2013 Category A7 - Missing Function Level Access Control
MemberOf	C	947	SFP Secondary Cluster: Authentication Bypass

▼ Notes

Relationship

This can be resultant from SQL injection vulnerabilities and other issues.

More information is available — Please select a different filter.

Page Last Updated: January 18, 2018



Use of the Common Weakness Enumeration and the associated references from this website are subject to the [Terms of Use](#). For more information, please email cwe@mitre.org.
CWE is sponsored by US-CERT in the office of Cybersecurity and Communications at the U.S. Department of Homeland Security. Copyright © 2006-2018, The MITRE Corporation.
CWE, CWSS, CVRAF, and the CWE logo are trademarks of The MITRE Corporation.

[Privacy policy](#)
[Terms of use](#)
[Contact us](#)

Figure 2-3: Example of a Vulnerability Disclosure Collected by CERT.

The key aspect of better and more secure information systems is the timely and reliable disclosure of security vulnerabilities such that the vendors can address the issues by patches and updates (Arora et al., 2003). However, the process of vulnerability disclosure is controversial and has been debated by practitioners and academics. Cavusoglu et al., (2007) argued that quick disclosure increases public awareness and puts

pressure on the vendors to issue patches quickly and, over time, results in better quality software. However, the availability of patches does not provide assurance that all users could be patched in time. Rescorla (2005) shows that public disclosure of the vulnerabilities could also enable criminals to use the information and take advantage of users who are unaware, or not able to patch in time. In the on-going debate on vulnerability disclosure, Arora et al. (2006) also showed that on an average both secret (non-disclosed) and disclosed (public but not patched) vulnerabilities attract fewer attacks than patched (disclosed and patched) vulnerabilities. They also find that attacks gradually increase with time after disclosure of patch release.

The economic incentives of vulnerability disclosure by a third party also raise concerns. One notable example is the practice of subscription-based vulnerability disclosures employed by security research firms. In such cases, the research firm is financially motivated to attract more “subscribers” by disclosing newly discovered vulnerabilities. To remain competitive, such firms are incentivized to disclose vulnerabilities as soon as possible and to as many subscribers as possible. Such practice raise the question of the potential damage due to malicious parties who would also have access to privileged information. The media coverage a security company receives can also mean substantial revenue in the form of new or larger customer contracts. Because of these hidden motives, the public is starting to question the true motivation behind some of the vulnerability research and disclosure. In some cases the vulnerabilities being disclosed by security firms are the result of intense stress testing of products (Tang et al., 2017). The likelihood of these vulnerabilities being discovered outside of a manufactured lab environment is

small. This poses the question as to whether these vulnerabilities should even be disclosed. For practitioners, the call for a generally agreed principal on vulnerability disclosure prompted the development of “Responsible Disclosure” (Shepherd, 2003). The key goal of responsible disclosure is to keep knowledge of vulnerabilities within the smallest circle of people until a patch can be developed and made public.

Although security breaches would invariably involve one or more vulnerability being exploited, the primary difference between vulnerability disclosure and breach disclosure is that vulnerability disclosures are usually made by third party researchers, not by the breached firm. In addition, the contents in vulnerability disclosure are the specific flaws of the system or software, often in the form of software codes. These disclosures do not involve the vulnerabilities of a firm’s ISM practices. The similarities between the two type of disclosure lies in the debate of externalities, on whether the need of the public knowledge could outweigh the need of private entities.

2.3.6 Automated Disclosure

Some breach disclosure may be performed automatically without additional human interaction. Unlike vulnerability disclosure, which usually involves third-party researchers or “whitehat” hackers using a proactive approach to investigate potential flaws before the vulnerabilities are discovered, automated disclosure is typically done after a security incident has occurred and is often collected by software or hardware vendors. The collected information typically includes logs and usage statistics that would be automatically delivered to the information collector. Automatical disclosure is used by

the hardware and software industry for collecting information on vulnerabilities by scanning or monitoring the system. For example, anti-virus and malware vendors usually collect such disclosures without user knowledge or express permission. This creates a potential security loophole for malicious attackers as such scans could immediately furnish a list of vulnerable users or systems that are affected by certain vulnerabilities, or systems that are not yet patched to the newest updates. Table 2-1 presents a summary of current disclosure practices.

Table 2-1: Summary of Current Breach Disclosure Practices

Type	Purpose	Timing	Content	Audience	Disclosed by
Internal Disclosure	To communicate the incident internally to management	Immediate upon breach	Detailed internal reports	Board members, senior management	Information system professional; internal auditor; system admin
Initial Disclosure	To inform regulator of the incident	*as fast as feasible	Summary of event	Regulator	Breached organization
Customer/individual Notification	To notify affected individuals or the breach	After impact evaluation	Nature of event, Impact analysis, remediation recommendations	Customers, affected individual	Breached organization
Periodic Disclosure	To summarize events that occurred during a period that may affect firm's economic conditions	Quarterly; Annually	Risk factor, impact on operations and on financial reporting	Investors; stock holders, financial statement users, regulators.	Breached organization and audited by third party auditors
Vulnerability Disclosure	To allow the development of software and/or controls	Before breach	Specific codes or steps to reproduce the flaw	Vendors, security researchers	Third party researchers, white hat hackers.
Automated Disclosure	To send exception reports to vendor	Immediate upon breach	Logs, statistics, and/or exception reports	Vendor	Software / hardware of the breached organization

*The timing of initial disclosure could vary depending on the regulations. The majority of breach disclosure requirements in the United States and Canada do not have a specific timeframe specified; however, in the EU, the timing of initial disclosure is set at 72 hours immediately upon the discovery of the breach.

2.4 Review of the Current State of Policies

Breach notification laws have significantly contributed to heightened awareness of the importance of information security throughout all levels of a business organization. In addition they have added to development of a level of cooperation among different departments within an organization that resulted from the need to monitor data access for the purposes of detecting, investigating, and reporting breaches (Burstein & Mulligan, 2007). Such laws and regulations often required mandatory disclosures of information surrounding a security breach; depending on jurisdiction, different geographical areas or industries may have different requirements on breach disclosure. For example, in a number of industries such as the financial sector and healthcare, there are guidelines and government compliance regulations that mandate strict disclosure practices.

One of the main goals of mandatory disclosure of security breaches is to inform the public and to reduce such crimes. Mulligan & Hoofnagle (2007) argues that security breach notification laws and statutes cause data collectors to internalize more costs associated with data loss. To avoid seeming like an irresponsible gatherer of data, organizations will seek to prevent unauthorized information disclosure by enhancing security investments aimed at minimizing risks of losing personal information. Furthermore, the initial hit that an organization suffers by having to disclose any security breach, regardless of its magnitude, may encourage organizations to protect more carefully the personal information under their control (Burstein & Mulligan, 2007).

Empirical evidence (Romanosky et al., 2011) also has shown that adoption of data breach disclosure laws reduce identity theft caused by data breaches, on average, by 6.1 percent.

2.4.1 United States: Complex, Overlapping Jurisdictions Spanning through Different Agencies and States

The majority of U.S. states have had legislative data breach reporting requirements for several years, and some are now beginning to update these requirements based on experience with the existing rules. At the Federal level, several bills have been put forward to set nationwide rules; however, none have passed to date. The most recent, a proposal by the White House, is entitled the U.S. Personal Data Notification and Protection Act. However, the U.S. has specific laws for the financial and health sectors that also contain breach reporting obligations for specific types of security breach.

1. Gramm-Leach-Bliley Act (GLBA) applies to the financial services sector;
2. Health Insurance Portability and Accountability Act (HIPAA) applies to healthcare, insurance, and medical industries;
3. Sarbanes-Oxley Act (SOX): applies to publicly traded firms to disclose "internal control deficiencies";

Gramm-Leach-Bliley Act (GLBA) and Enacting Interagency Guidelines

Title V of the Gramm-Leach-Bliley Act provided authority for each of the agencies governing financial institutions to establish and enforce guidelines to ensure the security of and protect against unauthorized access to or use of customer data. These agencies have issued two Interagency Guidelines requiring financial institutions to safeguard

personal data by developing reasonable security measures and requiring financial institutions to develop a formal response plan to deal with data security breaches (Department of Treasury, 2005). The security guidelines require that financial institutions conduct risk assessments where the particular security measures will depend on the risks presented by the complexity and scope of the business. They also require that financial institutions "consider, and adopt what is appropriate of, the specific security measures enumerated in the Guidelines, including access controls on customer information systems, background checks for employees, and incident response programs." Furthermore, the guidelines require financial institutions to monitor their service providers' compliance with these guidelines through contracts. The security breach program set up by the Interagency Guidelines has two aspects. First, the financial institution must immediately notify its oversight regulatory agency the moment a financial institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information (Department of Treasury, 2005). The Guidelines do not require that individual consumers be notified of a security breach unless, upon reasonable investigation, the financial institution determines that misuse of the customers' personal information has occurred or is reasonably possible to occur. The Guidelines, however, do not exempt information protected by encryption based on its encrypted status alone, because "there are many levels of encryption, some of which do not effectively protect customer information." (Department of Treasury, 2005).

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA was enacted in 1996 by the U.S. Congress, but implemented through regulations issued by the Department of Health and Human Services. These standards for protecting identifiable health information cover healthcare providers, health plans, healthcare clearinghouses (i.e., processors of health information), and business associates that contract with these entities to provide services that involve the use of health information. The standards regulate the manner in which identifiable health information, that is, any information that is created or received by a covered entity and relates to health condition, provision of health care, or payment for provision of health care and that identifies the individual, is protected and exchanged among covered entities. The standards set forth three sets of requirements regarding Administrative Safeguards, Physical Safeguards, and Technical Standards that cover standards that must be followed to ensure the security of identifiable health information, but are flexible enough to allow different entities to implement according to their specific characteristics.

Sarbanes-Oxley Act and Section 404 - Internal Controls Requirement

Sarbanes-Oxley section 404 requires companies that are registered under the 1933 Securities Act to build a sufficient system of internal controls "around the safeguarding of assets related to the timely detection of unauthorized acquisition, use or disposition of an entity's assets that could have a material effect on the financial statements." Because personal information gathered from employees, customers, and consumers and maintained in databases are unique assets for a publicly-traded company, protecting

personal information becomes a compliance requirement under Section 404. Public companies must disclose, in their annual filings, the system of internal controls that the company has in place to protect information and report inaccuracies, and must also attach an internal report of how the internal controls are working. Internal controls therefore "cover an enormous range of methods and procedures that an organization employs to ensure it is using resources as intended, preventing fraud, protecting assets from damage, and so on."(Ghose & Rajan, 2006) Penalties for non-compliance under Sarbanes-Oxley include possible criminal and civil prosecution, and monetary and criminal penalties.

State-level Regulations

At the State level, details of the legislation can vary from state to states, but the main principles are consistent: The laws require that affected individuals should be notified when their personal information has been lost or stolen. Specifically, the state laws usually require notification of (1) What happened, (2) What information was involved, (3) What steps and actions the breached organization have taken, (4) What actions can the affected individuals take, and (5) Contact information for additional inquiries.

One major issue regarding the different state laws is the condition, or threshold, at which public disclosures must be made. Among the 49 states that have established security breach notification laws, 25 state laws require notification "when the personal information is reasonably assumed to have been acquired by an unauthorized party, whereas other state laws require notification only if it is reasonable to believe the information will cause harm to consumers." However, the lack of a clear definition can

often lead to room for management discretion and misinterpretation. In addition, the consequences of not complying are not criminal. The enforcement includes civil right of action (the ability for affected consumers to bring a lawsuit) and many states do not specify a maximum civil penalty. In some states, (for example, Arizona and Arkansas) laws allow a civil penalty not exceeding \$10,000. The maximum is \$25,000 in Connecticut and Idaho, and \$500,000 in Florida (Romanosky et al., 2011). Compared to the potential market impact of a breach, it would appear that such penalties are of little consequence.

2.4.2 Canada - Still under Consideration by Government

There are two major pieces of legislation that govern security breach disclosure issues in Canada: the 2015 Digital Privacy Act and The Personal Information Protection and Electronic Document Act (PIPEDA). PIPEDA sets the rules for the collection, use and disclosure of personal information by organizations in the course of commercial activities. The Digital Privacy Act amended PIPEDA to require private sector organizations to notify Canadians in circumstances where their personal information has been lost or stolen, and they have been put at risk of harm as a result. In addition, organizations are required to report these potentially harmful data breaches to the Privacy Commissioner of Canada.

Subsection 2 of PIPEDA defines a "breach of security safeguards" as:

“The loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in Clause 4.7 of Schedule 1 or from a failure to establish those safeguards.”

It is worth noting that PIPEDA's definition of security breach is intended to include two elements - the first being that personal information is lost, or accessed by an unauthorized individual (either through theft or wrongful disclosure), and second, that the loss or unauthorized access is the result of someone violating the organization's security safeguards (or is the result of the organization failing to establish such safeguards). Therefore, under the Canadian PIPEDA definition, if a security breach does not involve the loss of personal information (for example, a DDOS attack on an organization's web applications), a breach notification would not be necessary.

In summary, organizations that experience a data breach - referred to in the Act as "a breach of security safeguards" - must:

1. Determine if the breach poses a "real risk of significant harm" to any individual whose personal information was involved in the breach;
2. Notify individuals as soon as feasible of any breach that poses a "real risk of significant harm";
3. Report any data breach that poses a "real risk of significant harm" to the Privacy Commissioner, as soon as feasible;
4. Where appropriate, notify any third party that the organization experiencing the breach believes is in a position to mitigate the risk of harm; and

5. Maintain a record of the data breach and make these records available to the Privacy Commissioner upon request.

In terms of enforcement, Canada's Digital Privacy Act provides for fines of up to CA\$100,000 for knowing violations of the breach notification requirements, or the requirement that organizations "keep and maintain a record of every breach of security safeguards involving personal information under [the organization's] control." Upon request, an organization will be obliged to produce this breach record to the Privacy Commissioner. Within Canada, currently Alberta is the only Canadian province with a mandatory breach notification requirement in effect.

2.4.3 European Union

The European Commission's ePrivacy Directive (European Commission, 2016) establishes breach reporting obligations on telecommunications service providers. Specific requirements under the Directive are set out in Commission Regulation (EU) No 611/2013. The European Union has published a draft General Data Protection Regulation which proposes to extend these requirements to all organizations.

Under the European Union's ePrivacy Directive, organizations are required to provide authorities with 17 different data points covering the identification of the organization; initial information on the data breach (such as date and time of breach and the nature and content of the personal information concerned); further information on the data breach (such as the number of individuals affected, a summary of the incident that caused the breach); possible additional notification to individuals (such as the content of the

notification and means of communication); and possible cross-border issues (such as notification to other competent national authorities

From 25 August 2013, European Commission Regulation 611/2013 (the Notification Regulation) sets out further rules about exactly how and when to notify, and what the notification must contain. Organizations must now notify the Information Commissioner's Office (ICO) of any personal data breach within 72 hours of detection.

2.5 Summary

This chapter started with a discussion of security breach definition, which illuminates the need to understand the type and different nature of breach that would warrant disclosure. After establishing a working definition of security breach, this chapter reviews current state of research, current practices, and current state of policies. In reviewing current literature, security breach disclosure studies and related literature on topics of disclosure in general are discussed. For current practices, different types of disclosure are compared. For the current state of policies, regulations from the United States, Canada, and the EU are reviewed to yield an understanding of what is required by the regulators. The following chapter focuses on more in-depth discussion on the theory and conceptual background of breach disclosure, which helps us to understand the economic driver for mandatory disclosure, voluntary disclosure, and management discretion in controlling disclosure.

3 Theory and Conceptual Background

3.1 The Economics of Disclosure

The economics of information security has recently become a thriving and fast-moving discipline and has attracted a new line of research in the development of theories and concepts. Anderson and Moore (2006) summarize four lines of research, 1) **misaligned incentives** – the moral hazard and adverse selection issue between the principle and the agent; 2) **Security as an externality** – where information security issues for one organization may have effects on others; 3) **Economics of Vulnerabilities** – this line of research investigates the issue of vulnerability disclosure issues and the economic consequences of vulnerability. 4) **Economics of Privacy** – this line of research investigates the notion that privacy is a commodity. Developments in these fields inform us that security failure is caused at least as often by bad incentives as by bad design. Due to misaligned incentives, systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail (Anderson & Moore, 2006).

Disclosure, particularly the disclosure of potentially damaging information regarding organizations, is an important aspect of business decision-making that has attracted the attention of the academic community. This line of literature has long and well-established theories that explore and explain the incentives, designs, and economic consequences of different types of disclosure under different circumstances. In information systems, the study of disclosure has not yet garnered much attention despite

the fact that this topic has burgeoned from a handful of papers on the topic to a substantial, and well-recognized, line of research such as the study of vulnerability disclosure.

The majority of IS research cites theories from social science and psychology to study the behavioral antecedents of individual actions and decisions. On the other hand, economics-based models of disclosure establish a link between information disclosure and the economic incentives, determinants, and consequences of that activity. It is crucial to understand the behavioral aspect of disclosure on an individual level. However, from the organizational level, without the “link”, or the economic motivation, research in security breach would be limited to individual motivations, rules and opinion promulgations, while the economic mechanism, arguably, the driver for business decisions, would be obscured or ignored.

3.2 Mandatory Disclosure

On the topic of mandatory disclosure, Frank H. Easterbrook and Daniel R. Fischel (1989) argue the necessity of mandatory disclosure. As they explained, disclosure entails externalities, i.e., a disclosing organization benefits not only itself, but also its peer organizations. The reason why mandatory enforcement is needed is due to the fact that the disclosing party endures all costs of disclosure but does not absorb all of its benefits, since actual disclosure levels may fall below the socially optimal ones. Therefore, policy makers have to take on the role of establishing mandatory disclosure rules detailing the

content, format, frequency, level of disclosure such that decision-relevant information are served to the decision makers in a timely manner.

The study of disclosure has a rich lineage in the economics literature. Perhaps the most notable works regarding disclosures is the “full disclosure” or “unraveling” studies of Grossman (1981), Grossman and Hart (1980), and Milgrom (1981). Generally, the literature is set in a Seller vs Buyer setting; however, the economics of the disclosure are generalizable in other contexts, if the assumptions hold. This line of literature states, that if (1) the buyers of a product know that a seller has information; (2) all buyers are reasonable persons, interpreting the sellers’ disclosures or nondisclosures in the same way, (3) the seller can credibly disclose the information he has received, and (4) the seller incurs no cost in making a disclosure, then the seller will always disclose his information. The reason is that any failure of the seller to disclose his information must be interpreted by buyers as implying that, if released, the information the seller has would cause the buyers to revise their perceptions of the value of the item sold. In order to value the item being sold correctly, buyers who are aware of the seller’s incentives must continue to revise downward their perceptions of the item’s value until the seller is better off revealing his information. This “unraveling” process predicts that organizations must disclose information to stay competitive. However, this process creates an enigma for the study of security breach disclosure. From the reported evidence from economic consequence studies (see chapter 2), we witness a common result that firms experience a financial setback subsequent to a security breach; this would be contrary to what the

unraveling process would suggest, at least for security breach disclosure, that the marketplace does not induce the firms to disclose.

From the security breach perspective, all of the above assumptions may be challenged. Security breaches have caught the public's attention due to recent media reports on large scale security breaches. However, it may not be the type of information that a well-informed individual might deem as important information that they must acquire, since the frequency of occurrence is still low on a per-organization basis. It is very possible that different information receivers may interpret security breach disclosure differently. The breached data, while adversely affecting the customer, might not directly affect the organization's ability to generate income, as shown by Ko and Dorantes (2006). Therefore, a disclosure of a security breach may induce very different reactions from a victim or a non-victim. In addition, the reaction from the information receivers may also differ in terms of their ability to interpret the information content in the disclosure. This would imply that information receivers would react differently if a security breach involves only the organization's own data, or if the breach has an impact on other users. Laube & Bohme (2016) argue that even under optimistic assumptions regarding the effectiveness of mandatory security breach reporting to authorities in reducing individual losses, it may be difficult to adjust the sanction level such that breach notification laws generate social benefit.

3.3 Voluntary Disclosure

Research on voluntary disclosure or discretionary disclosure examines how managers and/or organizations exercise discretion with regard to the disclosure of information about which they may have knowledge. The economic theory of voluntary disclosure has been discussed in the accounting and finance literature. The central premise of voluntary disclosure as stated by Dye (2011) is that *“the theory of voluntary disclosure is a special case of game theory... any entity contemplating making a disclosure will disclose information that is favorable to the entity, and will not disclose information unfavorable to the entity.”* From the security breach disclosure perspective, it would make sense that, if no mandatory rules exist, organizations that experienced security breaches would elect to avoid the exposure. In addition, if an organization has voluntarily disclosed such information, from the game theory perspective, the information user should anticipate the entity’s incentives to disclose the potentially damaging information.

Game theory sheds lights on how to interpret an organization’s actions surrounding the event. It permits us to investigate the incentives and evaluate the private information that is not observed. Consider an organization that heavily promotes a service that relies on user information and user privacy, but does not mention, or intentionally downplays, a security breach that involved the loss of customer information. Game theory permits us to infer that the organization’s product and its management is inferior. This is because if the organization’s product is superior, it will use the opportunity to disclose the organization’s insight over the matter. Case in point is the security breach to the Ashley Madison adultery web platform and Uber’s willful concealment of its breach. Also,

consider an organization that in the security disclosure repeatedly stresses and highlights offers of “free credit monitoring service”, for the affected customers but does not reveal information regarding the vulnerability that was exploited or its investigation effort. The theory permits us to infer that the organization’s attitude towards preventing future incidents might be questionable.

Therefore, if an organization voluntarily discloses or supply information above and beyond what is mandatorily required by the regulators, theory predicts that the organization is motivated to signal its value (Grossman & Stiglitz, 1976); providing a more detailed disclosure would therefore imply the organization expects potential benefits despite a higher cost to produce that signal.

3.4 Management Discretion and Control of Disclosure

Regardless of the type or the nature of disclosure, management could exert a certain level of control on the content, frequency, timing, and the extent of the disclosure. From the behavioral aspect, the manager or CEO may not want to be “the bearer of the bad news” or have his or her name associated with the bad news. From the agency theory perspective, management may wish to withhold bad news to minimize the impact on their incentive contracts (Kothari et al., 2009). For publicly traded firms, the issue of security breach disclosure could be much more nuanced due to the separation of ownership and control. Dye (1985) provided a simple analogy using agency theory showing that: Suppose the management’s actions are subject to moral hazard and hidden actions, and further suppose that investors, individually, learn about the manager’s actions through

disclosure that would reflect the management's action through stock price changes. Disclosure allows the firm's owners to mitigate the moral hazard problem by tying the manager's compensation to the firm's stock price, but in this case, the manager could game the system and make a disclosure sufficient to impact the firm's future cash flows. The firm's stock price would then become a function of that disclosure rather than a function of investor knowledge about the manager's actions. Dye's analysis highlights the particular issue of disclosure for public firms. In this case, subsequent to a security breach, managers may foresee that security breach events are intrinsically complex and difficult to understand for the principal; or it may take much longer for the full investigation to be completed. The manager may very reasonably elect to control the disclosure in a manner that favors the manager's self-interest such that the market reaction would be a function of the "diluted" disclosure, not the management's effort and their true action in managing or mis-managing the firm.

Existing studies on the disclosure of "bad news" also provide some insight explaining the managers' willingness to delay the security breach disclosure. Dogan et al. (2007) show that by delaying bad news, managers could make certain that the negative effect on firm performance could also be delayed. Dogan et al. (2007) also argue that delaying bad news basically means preventing the information from reaching the stakeholders. The second possible explanation is from the agency contract perspective in which managers having compensations or incentive contracts related to firm performance tend to delay unfavorable news until it is verified (Lurie and Pastena, 1975). Moreover, Graham et al.'s study (2005) reveals that one of the reasons for delaying the release of bad news is that

the company could further investigate and interpret the information content of this negative news. In terms of security breach disclosure, the area of information systems research could learn a great deal from these related studies in the economics, accounting, and finance stream this developing a better understanding of the economic motivations and drivers for disclosure.

4 The Elements of Security Breach Disclosure Requirements (RQ1)

4.1 Common Principles and Provisions for Disclosure

Surveying the security breach disclosure requirements from the United States, European Union, and Canada (See Chapter 2) there are notable differences between regulators on the following disclosure items:

1. The definition of reportable security incidents and security breaches.
2. The conditions for initial and public disclosure
3. The target audiences of the disclosure
4. The timing and deadlines of the report
5. The requirements of content on describing the nature of the event
6. The requirements on evaluating impact and assessing potential damage
7. The requirements on disclosing investigation and remediation efforts
8. Enforcement and penalties for non-compliance

The goal for mandatorily public disclosure regulation is to provide relevant parties a minimum set of relevant information. However, with multiple agencies and regulators in each state having different rules and requirements on disclosure, the reality of practice is difficult (Furnell & Thomson, 2009; Perlberg, 2014). This is because the affected parties may receive multiple notifications on one event at different times or the affected parties may receive differential treatment or disclosure due to residing in different regulatory

jurisdictions. Government regulators' roles are to enact laws and regulations to satisfy the public's right-to-know. However, due to the lack of research on what *should* be required and what *are* required, the scholarly community has not been able to advise policy and inform practice.

In this chapter, I explore the research question “*What are the common elements of security breach disclosure requirements?*” The goal of this research question is to generate a list of generalizable common elements of security breach disclosure elements that would be able to “answer stakeholders’ questions”. Such common elements could be used as the principle concepts for a more universal disclosure practice; however, the current momentum has shown that the regulatory requirements are becoming even more fractured and complex.

Scholars of government policies have begun efforts in finding the common provisions in breach disclosure laws. Notably, Sullivan & Maniff (2016) reviewed US state notification laws from 2006 to 2014 and determined 10 common provisions in security breach disclosures. The provisions are as follows:

1. **State Enforcement** allows the attorney general or another designated state entity to enforce organizational failures to comply with the statute.
2. **Risk of Harm** provisions require a breached organization to notify the affected parties only if the organization determines that the breach constitutes a reasonable likelihood of harm to the customer.

3. **Baseline Encryption Exemption** provisions exempt an organization from notifying consumers if the data stolen in the breach were redacted or encrypted.
4. **Notification Policy Exemption** provisions allow an organization that maintains its own notification procedures to be deemed in compliance with the state notification law so long as the organization does, in fact, disclose breaches.
5. **Notify AG/Credit Agencies** provisions require organizations to notify one or more parties, such as the attorney general or a credit reporting agency, when a breach occurs.
6. **Cap on Civil Penalty** provisions limit the financial civil penalty imposed on organizations found in violation of the statute.
7. **Doing Business in State** provisions specify that the notification law only covers organizations that conduct business in the state. In states without this provision, organizations that do not conduct business in the state are still required to notify if a customer whose personal information is breached is a resident of the state.
8. **Expanded Definition of Personal Information** provisions indicate whether the notification law covers more information than meets the standard definition of personal information (PI). States typically define PI as a first name or initial in combination with a last name and a Social Security number, driver's license number, state ID card number, or financial account number. An expanded definition of PI includes other personal data, most often health and medical information.

9. **Private Right of Action** provisions allow customers whose data were exposed to sue organizations for failure to comply with the data breach notification statute.
10. **Explicit Time Limit to Notify** provisions specify that organizations must notify affected customers within a given number of days (usually 30 or 45). Notification laws without a specific time limit require notification as quickly as possible and without unreasonable delay.

Sullivan and Maniff inspect the issue from the regulator's perspective, focusing their effort on what are the normative requirements that should be in place. However, their take on the viewpoint of the regulators is thus the result of their common principle and provisions that are focused on the relations and interactions between the breached organization and the regulators. In other words, their focus centers on the question of *"what needs to be designed into the regulation?"* This study furthers their efforts by taking a different approach. This is to inspect the major elements of security incidents while focusing on the relation and interactions between the breached organization and the information receiver through the question of *"what information surrounding a security breach would be relevant to the affected party?"* I approach this research question by focusing on the disclosure regulations and take particular notice of informational requirements that aim to satisfy the stakeholders' right-to-know. Using Grounded Theory Methodology (GTM), the informational requirements are then distilled into the common elements. The follow section explains the methodology and process.

4.2 Methodology

4.2.1 Use of GTM

To examine the common elements, I reviewed breach disclosure requirements from the United States, EU, and Canada employing GTM (Glaser & Strauss, 1967) coding techniques to extract salient information from the disclosure requirements. GTM is a relatively effective method for conducting exploratory research, especially in researching new phenomena and building new theoretical models of an organization's security breach disclosure practices. The term "Grounded Theory" refers both to a method of inquiry (examines the empirical reality through data) and to the product of inquiry (theories grounded on data). In this study, GTM is used for this specific mode of analysis. Essentially, GTM is a set of flexible analytic guidelines that enable researchers to focus their data collection and to build inductive theories through successive levels of data analysis and conceptual development (Charmaz, 2003). The major strength of GTM is that it provides a set of tools for analyzing processes systematically, which hold much potential for studying cybercrime issues. GTM encourages researchers to remain close to the empirical reality and develop an integrated set of theoretical concepts from empirical materials by not only synthesizing and interpreting them, but also showing processes and dynamic relationships that existing theories fail to predict or to explain.

GTM works by breaking down the data into small parts such as individual rows and then assigning tags, called codes, to each section. The construction of theory using GTM relies on a systematic analysis of empirical data to derive new knowledge, models, or theories. Therefore, the new knowledge obtained is grounded in evidence rather than

developed from existing conceptual frameworks or theory. This is particularly important in the study of complex phenomena such as security breach disclosures. *This study argues that other methodologies such as experiment, survey, or case studies are valid methodological approaches that would contribute to the scientific knowledge production. However, the study of security breach disclosure, due to its complex nature that involves multiple stakeholders and interlocking relations, requires systematic analyses of extant empirical data to produce relevant knowledge.* Using the security breach domains established by GTM, computerized textual analysis is then used to extract evidence. The use of computerized techniques is important, as it tends to lower the risk of bias and inter-coder validity concerns.

4.2.2 Data Source

I collected security breach requirements from all the following sources: U.S. state-level and federal-level, the EU, and Canada. In addition to breach requirements, I also collected industry best practices, surveys, and reports on security breach disclosure to be used for theoretical sampling. In terms of actual breach disclosure, I collected the California data security breach report from California Attorney General Office from 2012 to 2016. A subset of the breach disclosure reports are used to find the “question and answer” combo in this research that question the common elements, and in RQ2, where the full set of breach reports are used as the primary data source.

4.2.3 Conceptualization in GTM

In GTM, the conceptualization process refers to the analysis and “scaling up” of the “slices of data” to theoretical knowledge. From the “slices of data” extracted, GTM

specifies codes to represent the meaning. These codes are then compared, classified, and reorganized to “scale-up” and develop more abstract conceptual categories. This study follows the Glaserian (Glaser, 1999) approach to the grounded theory analysis method, emphasizing the induction or emergence of codes, concepts, categories that are rooted in data. To facilitate the iterative analysis and constant comparison technique, I use three stages of coding: opening coding, axial coding and selective coding for the conceptualization process. Throughout the coding processes, new codes, categories, and their relationships are constantly compared and analyzed in an iterative process. Therefore, notes and memos naturally emerge and highlight new insights or potential disagreements with existing theories or among researchers. This iterative analyses result in detailed memos that assist researchers in developing a theoretical understanding of the data and the process repeats until the point of *theoretical saturation*, in which the data do not reveal any new insights. Through this iterative and integrated process of data collection, analysis, coding, and conceptualization, an inductive theory about a practical area is generated (Putri et al., 2016). Figure 4-1 illustrates the Grounded Theory Method used in this study.

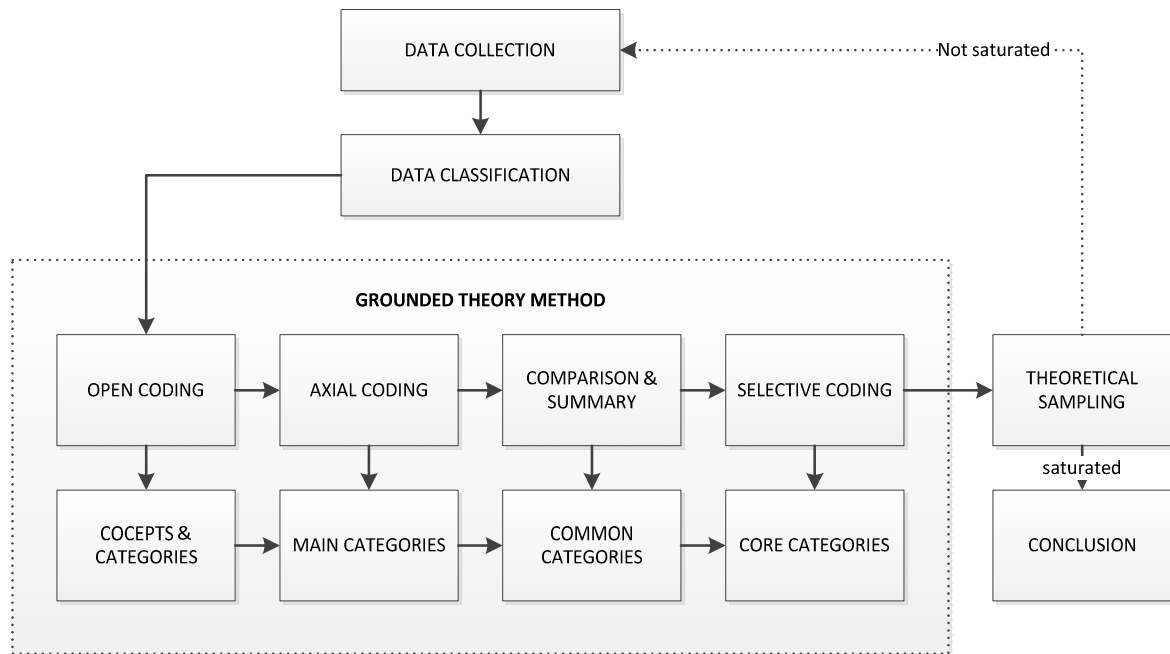


Figure 4-1: GTM Coding Processes

4.2.4 Coding Processes

I approached the open coding process with a very simplistic manner, taking a cue from California’s reader-centric approach, which aims to ask “simple questions in plain English” (California Civil Code s. 1798.29). In this way I classified requirements by the questions they would answer. Specifically, requirements were collected and coded with respect to how they would collect facts from the breached organization and answer a particular question the reader might have. In other words, I ask - “what is the question?” in the first open-coding process. The goal of the open coding process is to immerse the researcher in the data (Glaser, 1978); therefore, I approached the data with no particular design or theory in mind (*tabula rasa*). The questions were generic by design to avoid

legal or technical jargon. In addition, they are not driven by any prior knowledge in the domain of security management. Examples of these “questions” extracted from current regulations include:

- “What happened?”
- “Who is responsible?”
- “When did it happen?”
- “What was lost or damaged?”
- “What parties are involved?”
- “Were the authorities informed?”
- “What actions were performed by the organization?”
- “Does the incident require immediate action?”
- “Who should I contact?”
- “Who signed the disclosure?”

In GTM, the open coding stage is a process designed to expose the researcher to the full spectrum of data and not force the researcher to “filter” data into pre-defined conceptual categories; therefore, no effort at this stage was spent on conceptualizing the questionnaire-style of codes into higher level conceptual categories. Once the question was formulated, I searched the actual disclosure reports for the “slices of data.” The data quickly emerged and accumulated through the opening coding process and it became apparent that these loosely organized questionnaire-categories lacked structure and were just collections of Questions and Answers that lack meaning. The generic questions now

function as the initial categories or “collection bins” for the slices of data. The conceptual categories are then formulated through GTM’s iterative analysis process.

4.2.5 Axial Coding and The Interrelations of Main Categories

I continued the analysis on the relationships amongst categories and concepts defined from the open coding process. I then analyzed the causality conditions, dimensions and intermediaries of the phenomenon (Corbin & Strauss, 1990). During the axial coding process, multiple phenomena and concepts emerged as the main categories. Situational links between categories were made; these links were based on lower level category relationships (Urquhart, 2001). For example, when coding the source of attacker, “internal employee”, “contractor”, and “manager” emerged as potential candidates of categories, their actions that lead to the breach are then formed as the situational links to indicate the logical link to other categories.

The axial coding process centers on the needs to group and conceptualize the slices of data in a manner that highlights the logical relationship, i.e., a casual relation between categories. This is accomplished through focusing on the relevant verbs that signifies the “action”. This process helps to identify the logical flow of the main categories. For example, in the process of open coding, many potential sources are identified as the “who is responsible for the incident.” However, these sources could not successfully cause the breach if there is no weakness present in the system that allowed the breach to take place. In the axial coding process, such logical relations are identified.

4.2.6 Comparison of Categories and Scaling up to Common Categories

Constant comparison has been described as core to the grounded theory method (Charmaz, 2006). It is the process of constantly comparing instances of data that researchers have labeled as a particular category with other instances of data in the same category to see if these categories fit and are workable (Urquhart, 2001). One notable example of detecting such issues is the constant comparison of the data in the original category of “what happened?” During the constant comparison of instances of data in this category it became apparent that the category is too generic and contains multiple distinct conceptual categories within the loosely defined question. The conceptual category of threat agent, threat, and vulnerability is then distilled as the common category that would help distinguish the data. In this sense, the description of “what happened” would entail “who or what is responsible” (threat agent); “What is the nature of the incident (threat).

4.2.7 Selective Coding and Core Categories

Selective coding aims to develop the core categories that would explain the central phenomenon. The core category, as described by Glaser and Strauss (1978), categorizes the data that appear central to describing what is happening during breach disclosure. Using the grounded theory approach enables the study to pay special attention to the process flow between the components, thus illuminating the relationships between identified constructs. Therefore, the core categories encompass a flow of different, but common elements in all breach disclosures. In this sense, the logical relation is now

identified as depicted in Figure 4-2, that THREAT AGENT – (gives rise to) THREAT – (which exploits) – VULNERABILITY – (that leads to) – SECURITY BREACH.

4.3 Elements of Security Breach Disclosure

Through the review and use of the grounded theory coding technique, I identified the common elements as information about *threat agents*, the *threats*, the *vulnerability*, the *discovery* of the incident, the *investigation*, the potential *impact*, and the *remediation* actions. These elements provide the baseline information of the security breach to the party affected. Therefore, these elements are used as seed concepts in guiding the analysis and the extraction of “data snippets” from the data. Figure 4-2 depicts the essential seven elements surrounding security breaches.

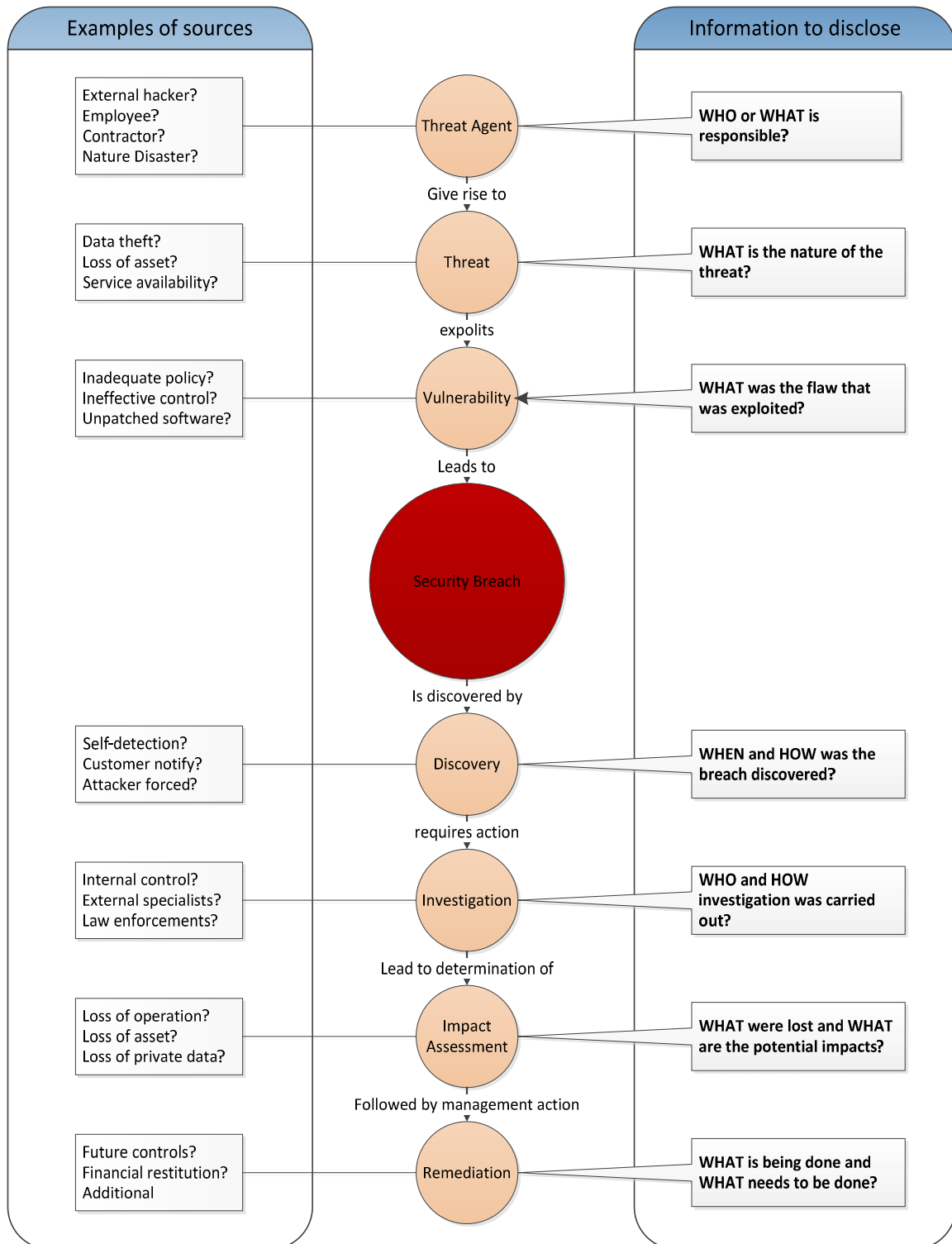


Figure 4-2: Common Elements of Security Breach Disclosure

4.3.1 Disclosure of Threat Agent, Nature of The Threat, and Vulnerabilities

Threat Agent

The term *Threat Agent* or *Threat Actor* is used to indicate an individual or a group that can manifest a threat to the confidentiality, integrity, and availability of system resources (Bowen et al., 2007). Under the NIST (National Institute of Standards and Technology) definition, anyone and anything can, under the right circumstances, be a threat agent. This would include external hackers, or well-intentioned, but inept, employees or even nature elements such as a large-area flood that would destroy stored data. (NIST 800-53, 2012).

Threat agents can take one or more of the following actions against an asset (NIST 800-53, 2012):

- Access – unauthorized access
- Misuse – unauthorized use of asset
- Disclose – the threat agent illicitly discloses sensitive information
- Modify – unauthorized changes to an asset
- Deny access – includes destruction, blocking authorized access, etc.

It's important to recognize that each of these actions affects various assets differently. Actions and their ability to affect the assets drive the different natures of the threat. For example, the potential for productivity loss resulting from a destroyed or stolen asset

depends upon how critical that asset is to the organization's productivity. If a critical asset is simply illicitly accessed, there is no direct productivity loss. Similarly, the destruction of a highly sensitive asset that doesn't play a critical role in productivity won't directly result in a significant productivity loss. Yet that same asset, if disclosed, can result in significant loss of competitive advantage or reputation, and generate potential legal costs. The point is that it's the combination of the asset and type of action against the asset that determines the fundamental nature and degree of loss. Which action(s) a threat agent takes will be driven primarily by that agent's motive (e.g., financial gain, revenge, recreation, etc.) and the nature of the asset. For example, a threat agent bent on financial gain is less likely to destroy a critical server than they are to steal an easily pawned asset like a laptop.

The Open Web Application Security Project (OWASP) defines threat agent in its Application Security Guide for CISO Project (OWASP, 2012) as:

$$\textit{Threat Agent} = \textit{Capabilities} + \textit{Intentions} + \textit{Past Activities}$$

Using OWASP's definition, only humans can be threat agents. Another important distinction of OWASP's definition is the inclusion of "Intention" - this would exclude accidental security incidents or nature disasters from potential threat agents. This study adheres to NIST's definition as threats to the confidentiality, integrity, and availability of system resources that can be caused by not only criminals with the intention to commit crime, but also careless employees or Mother Nature.

4.3.2 Disclosure on Detection, Discovery, and Investigation

Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices (Scarfone & Mell, 2007). Detection controls in a sound, adequate control environment should be composed of several types of components, including human, in the form of administrative controls, or technical agents, in the form of technical controls. The purpose of the disclosure on detection is such that the timing of the intrusion and the timing of the discovery can be reported to the relevant parties. The time lag between incident time and discovery time could be an important indicator of how well the detection controls are working. Without such disclosure on detection, the breach disclosure would not be able to communicate the following information content to the relevant stakeholders:

- The timing, mean, and method of the intrusion.
- How long does it take for the organization to respond?
- What actions are taken immediately upon the discovery of the intrusion?
- What parties are involved in the discovery and investigation process?
- What resources, such as independent digital forensic investigators or law enforcement services, are involved?

4.3.3 Disclosure on Risk Assessment and Impact Analysis

The disclosure on risk assessment and impact analysis allows relevant stakeholders to learn about what are the potential impacts of the loss. The information contained in the risk assessment and impact analysis allows decision makers to assess the criticality of the event and to prioritize the handling of the incident.

NIST's Computer Security Incident Handling Guide (Cichonski et al., 2012) suggests that impact of a security breach should be evaluated according to the following:

- a) **Functional Impact of the Incident.** Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems. Incident handlers should consider how the incident will impact the existing functionality of the affected systems. They should also consider not only the current functional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained.
- b) **Information Impact of the Incident.** Incidents may affect the confidentiality, integrity, and availability of the organization's information. For example, a malicious agent may exfiltrate sensitive information. Incident handlers should consider how this information exfiltration will impact the organization's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertained to a partner organization.

- c) **Recoverability from the Incident.** The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances it is not possible to recover from an incident (e.g., if the confidentiality of sensitive information has been compromised) and it would not make sense to spend limited resources on an elongated incident handling cycle, unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an incident may require far more resources to handle than what an organization has available. Incident handlers should consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.

Combining the functional impact on the organization's systems and the impact on the organization's information determines the business impact of the incident—for example, a distributed denial of service attack against a public web server may temporarily reduce the functionality for users attempting to access the server, whereas unauthorized root-level access to a public web server may result in the exfiltration of personally identifiable information (PII), which could have a long-lasting impact on the organization's reputation. The different types of impact may also assist the relevant stakeholder in understanding whether the breach would introduce potential vulnerabilities in the future and take actions accordingly.

4.3.4 Disclosure on Remediation, Containment, Corrective Control, and Preventive Controls

Containment, corrective controls, and preventive controls are important elements in the disclosure that communicate that the organization is on top of the breach and able to contain, correct, and set up controls to prevent future incidents. From the disclosure, relevant stakeholders would be able to learn the decisions and actions in dealing with incidents and develop strategies accordingly.

Disclosure for containment, corrective and preventive controls post-incident may include the following (Cichonski et al., 2012):

- Actions to prevent potential damage to and theft of resources.
- Actions for evidence preservation.
- Actions to preserve service availability (e.g., network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partial containment, full containment)
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

4.4 Usage Example of the Common Elements

This following example shows the use of the common elements to extract information from actual disclosure reports. From each disclosure, the sentences are used as the unit of analysis and extracted if one satisfies any of the seven disclosure elements (threat

agent, threat, vulnerability, detection, investigation, and remediation). The extracted sentences, which represent the existence of information content, can then serve as evidence of compliance or can be used for further analysis. Applying this rule, a single sentence, which contains multiple elements of disclosure, could satisfy as evidence for compliance. For example, the following sentence:

*“On January 29, 2015, Anthem, Inc. (Anthem) **discovered** that **cyber attackers** **executed** a sophisticated attack to gain **unauthorized access** to Anthem's IT system and obtained personal information relating to consumers who were or are currently covered by Anthem or other independent Blue Cross and Blue Shield plans that work with Anthem.”*

The sentence contains the following information on threat agent (cyber attackers); threat (unauthorized access to IT system and personal information); detection (On January 29, 2015, Anthem, Inc. (Anthem) discovered...) Therefore, it would satisfy the compliance requirements for three elements.

4.5 Summary

This chapter starts the investigation of research question 1 - focusing on the current disclosure regulations from various agencies in the US, EU, and Canada with the objective of establishing the common elements of disclosure. Through the review and use of the grounded theory coding technique, I identified that the common elements are information about *threat agents*, the *threats*, the *vulnerability*, the *discovery* of the incident, the *investigation*, the potential *impact*, and the *remediation* actions. These elements are distilled through a thorough review of existing policies and assisted by

GTM coding processes; they provide the baseline information about the security breach to the party affected.

5 The Information Content of Security Breach Disclosure (RQ2)

5.1 Extracting Information Content from Unstructured Breach Reports

In order to understand and analyze the information content of security breach disclosures, the information must be first extracted and organized. The information extraction process, as defined by Cowie and Wilks (1996), is the process which “*selectively structures and combines data which is found, explicitly stated or implied, in one or more texts.*” Each security breach disclosure is, by default, unstructured data, which means the information contained in the disclosure does not have a pre-defined data model and is not organized in a pre-defined manner. It is primarily descriptive, text-based data but may also include tables, graphics, and forms. Relevant information, as it is not ordered in any particular fashion may therefore be scattered throughout the entire disclosure report. The plain-text portion of the report, as it does not have any particular data type and may contain data such as dates, numbers, named entities, and logical inferences, therefore requires an information extraction process that will extract and structure the data in a meaningful way. The irregularities and complexities of natural language make it difficult to process disclosures using traditional computer programs as compared to data stored in structured form in databases or annotated (semantically tagged) in documents. Such an unstructured manner in presenting data is to be expected as data structures do not yet exist for disclosures. Only through repeated practice or improved understanding would

an intrinsic structure emerge. Understandably, the current unstructured presentations makes it difficult to evaluate or to compare the information content.

There are many existing techniques to turn unstructured data into structured data for analysis. Manually, one could employ GTM, as presented in the previous chapter, and use its well-defined coding processes to extract data snippets that have particular theoretical meanings to the researcher. One could also use computer-assisted techniques such as data mining, natural language processing (NLP) tools, and statistical analytics to find patterns or interpret the disclosure data.

5.2 Extraction Approach

Common techniques in structuring text usually involve manual tagging with metadata (GTM) or computerized part-of-speech tagging for further text mining-based structuring. Computerized approaches enable the researcher to process large volume of text data very quickly; however, pattern of categories or the hierarchy or the taxonomy structure can be difficult to determine via computer alone. Although recent progress in AI (Artificial Intelligence) has made significant improvements in pattern recognition, it still requires a “learning” process to train the computer programs first. (Michalski et al., 2013). On the other hand, using GTM, the researcher must become immersed in the raw data before the structure will “naturally emerge” through constant comparison iterative analysis (Glaser, 1978). There are advantages and disadvantages in either method. Human processing, with either single researchers or researcher groups, are able to achieve high theory sensitivity and are able to extract the semantic meaning from the text much better than

relying on machines alone. However, human processing on large volumes of text is very time-consuming and the rigor of GTM is prone to reliability or inter-validity issues (Gasson, 2004). On the other hand, advances in textual analysis software allows researchers to extract machine-readable information utilizing linguistic, grammatical, and visual structures that exist in all forms of human communication (Aggarwal & Zhai, 2012). Algorithms can infer this inherent structure from text, for instance, by examining word morphology, sentence syntax, and other small- and large-scale patterns (Berry, 2004). Through advancements in text-mining techniques, categories can be inferred through dimension reduction or cluster analysis (Ding & He, 2004), if there is a reasonable large sample of text to perform such analysis.

Through computerized processing, or “tagging”, unstructured breach information can be transformed to address ambiguities. Relevancy-based techniques can then be used to facilitate regression analysis and discovery. (Faircolough, 2003). However, text-mining itself has little theory sensitivity and relies on the text to extract semantic meanings. It is thus unable to “read between the lines” to extract meaning from the text. In this study I used the approach of combining the grounded theory method with textual analysis techniques to extract and classify data. Table 5-1 presents a summary of different research concerns when undertaking computer and human processing of text.

**Table 5-1 Research Concerns in Using Human vs Computer for Knowledge
Extraction**

Research Concerns	Human - Single Researcher	Human - Research Group	Computer Extraction + Human	Text-mining
Theory Sensitivity	HIGH	mixed	HIGH	none
Semantic Meaning	HIGH	HIGH	mixed	none
Sample Size	low	medium	medium	HIGH
Conceptualization	HIGH	medium	medium	none
Extract meaning	HIGH	medium	HIGH	none
Time Requirement (Researcher)	HIGH	medium	HIGH	medium
Time investment (Total)	medium	HIGH	medium	low
Costs	\$\$\$\$	\$\$\$	\$\$	\$

5.3 Data Source

Security breach disclosure reports were collected from the California Attorney General's Office, which covers reports from 2012 to 2016. All reports are available on the Attorney General Office's website and can be downloaded by anyone. The State of California requires a business or state agency to notify any California resident whose unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person. The mandatory disclosure requirement specifies that any person or business is required to issue a security breach notification if more than 500 California

residents have been affected by a single breach of the person's or business's security system. A single sample copy of that security breach notification, excluding any personally identifiable information, shall be electronically submitted to the Attorney General.

Breach data from the California Attorney General's office has the following characteristics:

- The reportable security breach is defined as “*unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person*” with a criterion of affecting “*more than 500 California residents*” from a single breach. Therefore, the security breach reports in this sample only contain breaches that satisfy this definition.
- The breach report could come from many types of entities. The source may include individuals or businesses, private or public, and may come from various industries that deal with personal data.
- With respect to California's disclosure requirements, there is no difference between the disclosure to the regulator and the disclosure to the affected individuals. Per the disclosure requirements, breached organizations should “*electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General.*” Therefore, the breach disclosure to the regulator is, in essence, a copy of the notification letter to the victims of the breach.

The final sample contained 859 cases and 1,544 reports, with the average breach report consisting of 646 words.

5.4 Methodology

5.4.1 Information Extraction and Parsing Unstructured Disclosure Reports

The “parsing stage” of information extraction, as described by Cowie and Wilks (1996), handles the “ecology of natural language” and identifies proper name identification and classification. Typically, numbers (in text or numeric form), dates, and other regularly formed constructions are also recognized in this stage. As suggested by Cowie and Wilks, the process involves the use of case information, special lexicons, and context free patterns, which can be processed rapidly in the first pass. Often a second pass may be required to confirm items that cannot be reliably identified by the patterns, but which can be flagged more reliably once fuller forms of syntactic relations are identified. (Chomsky, 2002)

To develop the special lexicon and case information for the classification, the data from processed security breach reports were extracted using the following steps:

- **Sentence Segmentation:** the raw text of the disclosure is split into sentences using a sentence segmenter;
- **Tokenization:** each sentence is further subdivided into words using a tokenizer;
- **Part of Speech Tagging:** each sentence is tagged with part-of-speech tags such as noun, verb, etc.;

- **Named Entity Recognition:** search for mentions of recognized entities in each sentence, accomplished by lexicons;
- **Syntactic Relation Recognition:** search for likely relations between different entities in the text.

From the extracted sentences and POS tags, this study then manually uses the common elements learned in RQ1 to determine if the extracted “actions” fit what is defined in the element. This allows the researcher to identify part-of-speech (POS) elements that are relevant to the seven possible elements. Using human ability to interpret the semantic meaning of the sentence and then build special lexicon to assist in classification of the text allows information to be efficiently extracted from each report. This includes the nature of the breach, who is responsible for the breach, when and how the breach was discovered, what type of information was compromised, what actions were taken after the breach was discovered, etc. Linguistic rules represented by regular expressions can be used to capture certain types of information. For example, general named entities such as time, person, organization, location can be recognized. Specific named entities also can be recognized by a pre-specified ontology such as data type which could be customer name, credit card number, social security number etc. Name entity recognition allowed this study to identify how many details are given within a sentence.

Using the ARK syntactic & Semantic parsing tool from Carnegie Mellon University (<http://www.cs.cmu.edu/~ark/>), the sentences were analyzed through a lexicon that defines the category of the actions. Figure (5-1) shows the process described above:

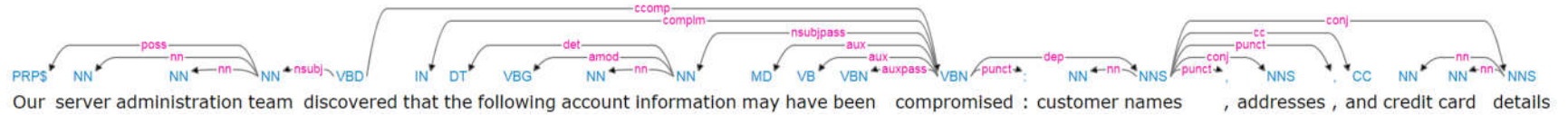


Figure 5-1: Visualization of Part of Speech Tagging and Syntactic Dependency Information from a Breach Disclosure.

The tokenized synaptic relationship analysis provides the following information:

1. This sentence provides information about “**discovery**”
2. “*Our server administrator team*”, a composite noun is responsible for the discovery
3. “*That the following account information may have been compromised: customer names, addresses, and credit card details*” the phenomenon that was discovered
4. The following information **may**” indicates a hypothetical event, indicates uncertainty and ambiguity.
5. The threat was “account information may have been **compromised**”
6. The named entity in the subject shows that “**customers names, addresses, credit card numbers details** are related to “**compromised**”
7. The sentence indicates the existence of information on “**discovery**” and information on “**threat**”

Semantic relations can be recognized by syntactic patterns. For instance, a named entity (person|organization|system) followed by the discovery action verb (detected|discovered|notified|found|informed) indicates the agent who discovered the incident. In the same vein, the named entity (person|organization|system) followed by the exposure action verb (compromised|exposed|stolen|misused|lost) would indicate the types of data being compromised. In addition to the tools available from the ARK project at Carnegie Mellon University, the study also used the Python open source software package, Natural Language Toolkit (Bird et al. 2009), to perform information extraction and lexicon building.

5.4.2 XML Tags and Structure

One of the most prominent examples of transforming unstructured data to structured data is the use of eXtensible Business Reporting Language (XBRL), through which organizational annual reports are communicated and stored in structured documents with semantic meaning. XBRL is XML-based and uses the XML syntax and related XML technologies such as XML Schema, XLink, XPath, and Namespaces.

The use of XML allows organization to employ a standards-based way to communicate and exchange breach information between different entities. These communications are defined by metadata set out in taxonomies, which capture the definition of individual reporting elements as well as the relationships between breach elements and other semantic meanings. The benefit of XML and XBRL is commonly recognized by both SEC and academics (Debreaceny & Gray, 2001; Pinsker & Li, 2008; Yoon et al., 2011).

However, there has been no such effort in collecting or presenting security breach reports using a structured reporting system. This study marks the first attempt to establish a structured taxonomy in security breach disclosure through manual analysis.

After the extraction process, each breach report would be accompanied by an XML document with a structure shown in Figure 5-2. The seven main categories are contained in the root <disclosure> tag, which contains the <id>, <organization_name>, <industry_sector>, <meta_properties> and various data extracted from the disclosure. Within each of the seven element tags, there can be multiple expandable <ident> tag to indicate multiple instances of discovered evidence. For example, Figure 5-3 shows multiple parties are involved in the investigation effort. In this case, there are two <ident> tags to indicate that more than one unique instance is logged.

Each <ident> tag may also contain multiple <desc> tags, where each <desc> tag is the original sentence extracted from the disclosure document. There could be more than one sentence describing each unique <ident> tag. For example, one organization may discover “Breach of confidentiality to personal data” as the threat; however, the organization may choose to describe the threat using more than one sentence, resulting in multiple <desc> tags in one <ident> tag. Appendix 4 shows an example of a complete XML document after extraction.

```

.....10.....20.....30.....40.....50.....60
1  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2  <disclosure>
3      <type></type>
4      <organization_name></organization_name>
5      <file_date></file_date>
6      <id></id>
7      <threat_actor>
8          <ident>
13     </threat_actor>
14     <threat>
15         <ident>
20     </threat>
21     <vulnerability>
22         <ident>
27     </vulnerability>
28     <discovery>
29         <ident>
35     </discovery>
36     <investigation>
37         <ident>
43     </investigation>
44     <impact_assessment>
45         <ident>
50     </impact_assessment>
51     <remediation>
52         <ident>
58     </remediation>
59     <other>
60         <contact></contact>
61         <apology></apology>
62         <signed></signed>
63         <timeref>
69     </other>
70 </disclosure>

```

Figure 5-2: Breach Disclosure XML Document Base Structure


```
<investigation>
<ident>
  <date>October 12th, 2016</date>
  <by>Self</by>
  <desc>The intrusion happened during an upgrade to kp.org that
    occurred at 11:26 p.m. Pacific time on October 12th, 2016</desc>
</ident>
<ident>
  <date>October 15th, 2016</date>
  <by>FBI</by>
  <desc>On October 15th, 2016, we contacted FBI cybercrime unit for
    further assistance</desc>
</ident>
</investigation>
```

Figure 5-3: Expanded <investigation> Tag with Multiple Instances of Investigation Evidence

5.4.3 From Semi-structured Data (XML) to Database (Structured Data)

Once data are transformed into XML, it can be presented in multiple output formats. For statistical analysis, the XML data for each disclosure can be funneled into a relational database for further analysis. In addition, using the developed structure, developers could also design web-forms that would store not only the disclosure source pdf document, but also collect information directly from the stakeholder through an XML-enabled form.

5.5 Descriptive Analysis

To provide a bird's-eye view of the data, first I developed in Python a computerized text processing tool to collect meta properties such as the year, sentence counts, word counts, disclosure delay, and the industry sector from the disclosure reports. Meta properties do

not reveal many insights on the subject matter; however, with the accumulation of data, the meta properties allow us to see the trends and observe the phenomenon from a high level. This helps us to understand the phenomenon and explore the issue further. Table 5-2 presents a summary of the breach reports analyzed by year.

Table 5-2: Breach Report Properties by Year

<i>Year</i>	<i>Reports</i>	<i>Percentage</i>	<i>Sentence Count</i>	<i>Word Count</i>	<i>Average Reporting Delay (days)</i>
2012	126	15%	36.38	682.12	80.83
2013	161	19%	30.67	593.83	113.88
2014	179	21%	34.75	650.13	164.64
2015	202	24%	33.22	649.62	201.76
2016	189	22%	36.44	657.51	187.25
All Years	857		34.29	646.64	149.67

From Table 5-2, it can be seen that the security breach disclosures have been on a steady increase since first introduced in 2012. Using a simple linear regression model regress number of reports, word counts, and average delay on year, the results shows that of number of reports are increasing (t-value: 10.03; adjusted-R square: 0.97). Figure 5-4 represents the fit plot for number of reports from 2012-2015.

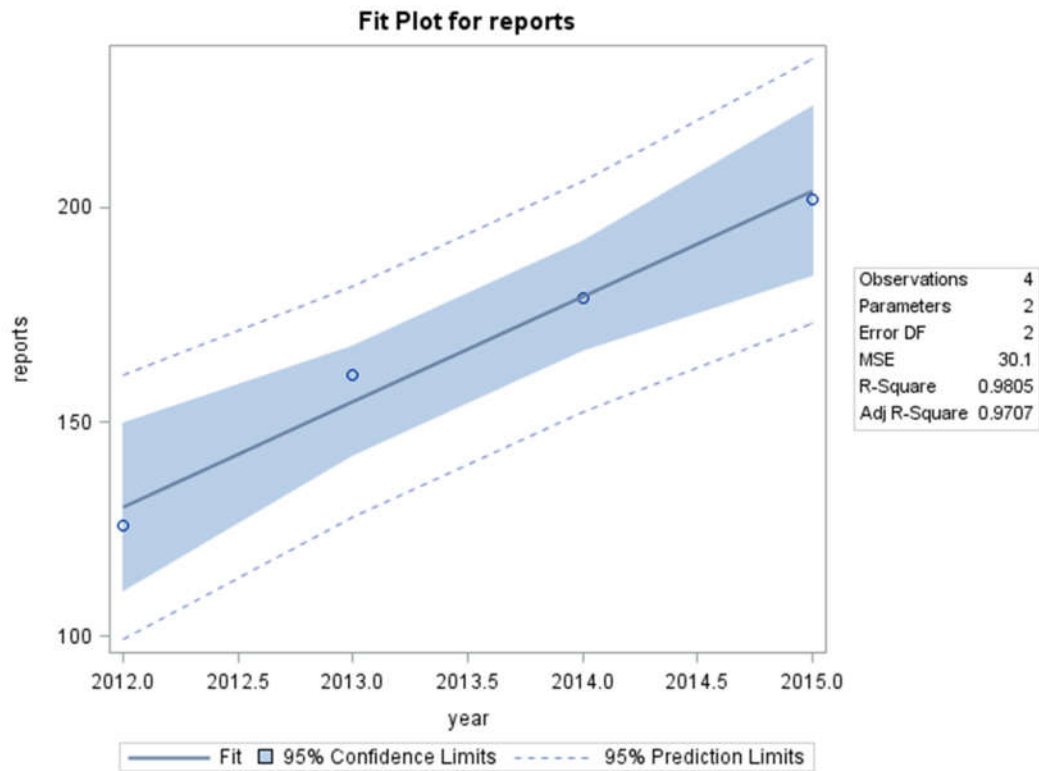


Figure 5-4: Fit Plot for Number of Disclosure Reports (2012-2015)

For year 2016, the sample only contains breach disclosures until and including the month of September. However, based on the linear regression result, it is reasonable to expect that the total number of disclosures in 2016 will exceed the total disclosures in 2015. On the other hand, in the first year of the disclosure requirement (2012), the data shows that organizations generally invest more effort in the disclosure in the form of providing longer reports (average 46 sentences and 682 words) while in 2013, the second year, both sentence counts and word counts have decreased (paired t-test p-value < 0.01). One possible explanation is that during the first year introduction of the law, there are certain expectation and assumptions of how non-compliant organizations would be penalized. However, determining non-compliant cases can be difficult and on the other hand, the

terms of penalties are also very ambiguous; therefore, it is reasonable to expect that effort toward compliancy requirement would decline after the first year. It can be observed the decline is shown not only through the decreased content, but also through the average disclosure delay observed. In 2012, the average reporting delay is 80.83 days, however, the average reporting delay has become longer and longer since 2012. The longest average delay was observed in 2015, where the average disclosure lag was 201 days. This indicates that affected parties did not learn about the security breach until more than half year later. Using linear regression model regressing disclosure delay on year, the results shows the increase in delay since 2012 is statistically significant (t-value: 17.92; adjusted R-square: 0.9907).

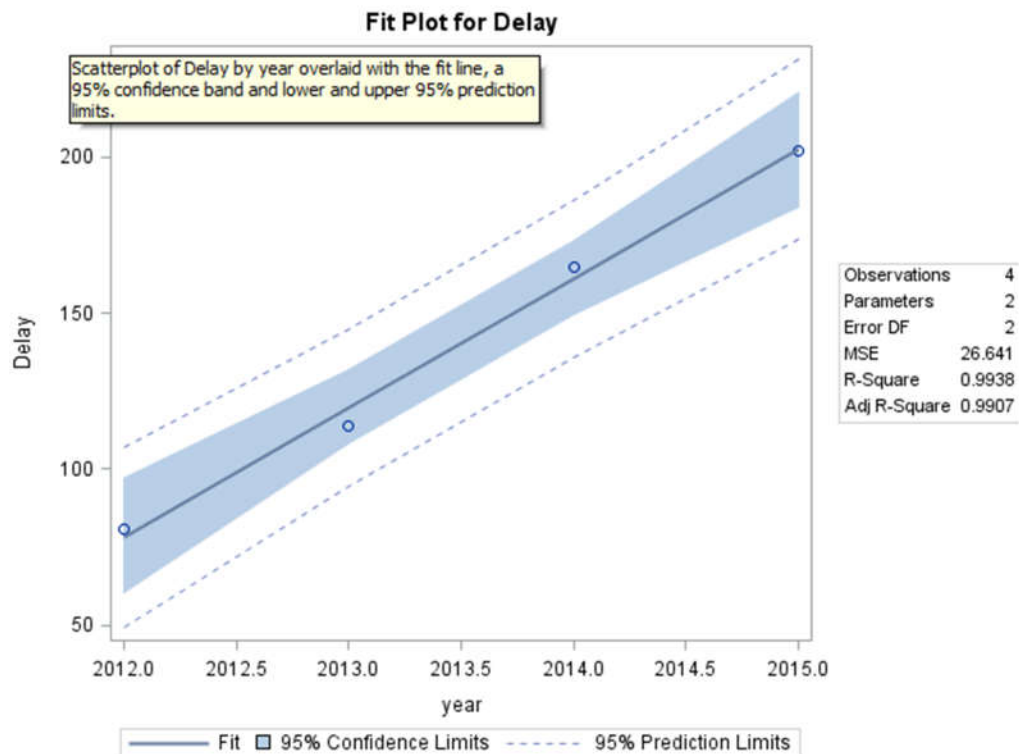


Figure 5-5: Fit Plot for Disclosure Delay (2012-2015)

From the industry analysis (Table 5-3), out of the total of 859 cases, 41% are from the financial and medical industries. However, this does not necessarily mean organizations from financial and medical sector suffer more security breaches than other industries. It is very likely due to security breach disclosure requirements for the financial (GLBA) and the medical (HIPAA) industry are already in place. Both breach disclosure requirements are quite mature and breach disclosure are required on a national level; therefore, it does not take additional effort for organizations to prepare disclosures for the State of California. However, the fact that 41% of disclosures are from the two industries also could be a warning sign that other industries, without existing compliance requirements, could be lacking in truthfully disclosing security breaches. However, this is very difficult to prove whether breaches were either non-existent or intentionally withheld. By the same token, it is also very difficult to prove that organizations in the financial and medical industries do suffer more security breaches than organizations in other industries if such incidence were never reported or intentionally withheld.

Table 5-3: Breach Report Properties by Industry

<i>Industry</i>	<i>Reports</i>	<i>Percentage</i>	<i>Sentence Count</i>	<i>Word Count</i>	<i>Average Reporting Delay (days)</i>
Education	7	1%	35.29	668.57	89.5
IT	29	3%	29.54	525.63	103.2
Communications	4	0%	31.75	567.50	39.5
E-commerce	27	3%	30.07	550.04	146.2
Education	35	4%	35.91	699.89	80.6
Financial	192	22%	38.12	715.62	275.8
Hospitality	76	9%	29.67	632.41	188.4
Insurance	21	2%	33.62	662.19	245.5
Manufacturing	31	4%	46.65	742.13	170.4
Medical	165	19%	30.95	589.52	142.0
Others	39	5%	34.40	629.20	84.5
Public	27	3%	25.04	511.48	52.6
Retail	71	8%	37.46	726.49	108.2
Service	135	16%	34.09	644.92	106.2
All	859		34.31	646.64	149.67

5.6 Analysis of what are contained in breach disclosures

Using the extraction method described in Section 5.4, information content of disclosure reports categorized by the seven common elements were extracted and stored in XML form. From XML, the raw data were then stored in a relational database for further analysis. Sentences used to describe each of the seven common elements were stored as

raw evidence in the XML document. Table 5-4 presents the sentence count based on the common elements extracted.

Table 5-4 Breach Report Common Elements (sentence counts)

<i>Common Elements</i>	<i>Maximum</i>	<i>Mean</i>	<i>Median</i>	<i>Minimum</i>	<i>Std Dev</i>
Threat Agent description - Internal	7	0.18	0	0	0.65
Threat Agent description - External	11	1.03	0	0	1.59
Vulnerability description	3	0.26	0	0	0.5
Threat description	14	3.07	3	0	2.56
Detection Description	13	1.39	1	0	1.78
Investigation description	16	3.3	3	0	2.5
Impact description	21	3.16	3	0	2.38
Remediation description	10	1.91	2	0	1.6

It can be seen that on average, organizations tend to exert more effort on describing external threat agents but less on internal threats. Also, it appears that very little effort was exerted to describe vulnerability, which describes what weaknesses were exploited that lead to the breach. On average, only 1 out of 4 breaches (0.26) included a vulnerability description. This is very alarming as it shows, on the disclosure reports, that organizations are more eager to allocate the blame instead of reviewing what weakness lead to the breach. Overall, the data show a wide disparity of information content on what are disclosed. Through the boxplot presented in Figure 5-4, it can be seen that the majority of the reports include less than 5 sentences on any of the common elements while some extreme cases with detailed descriptions skewed the average. This

disparity and distribution of coverage is concerning as it shows that the majority of organizations performed poorly in providing details.

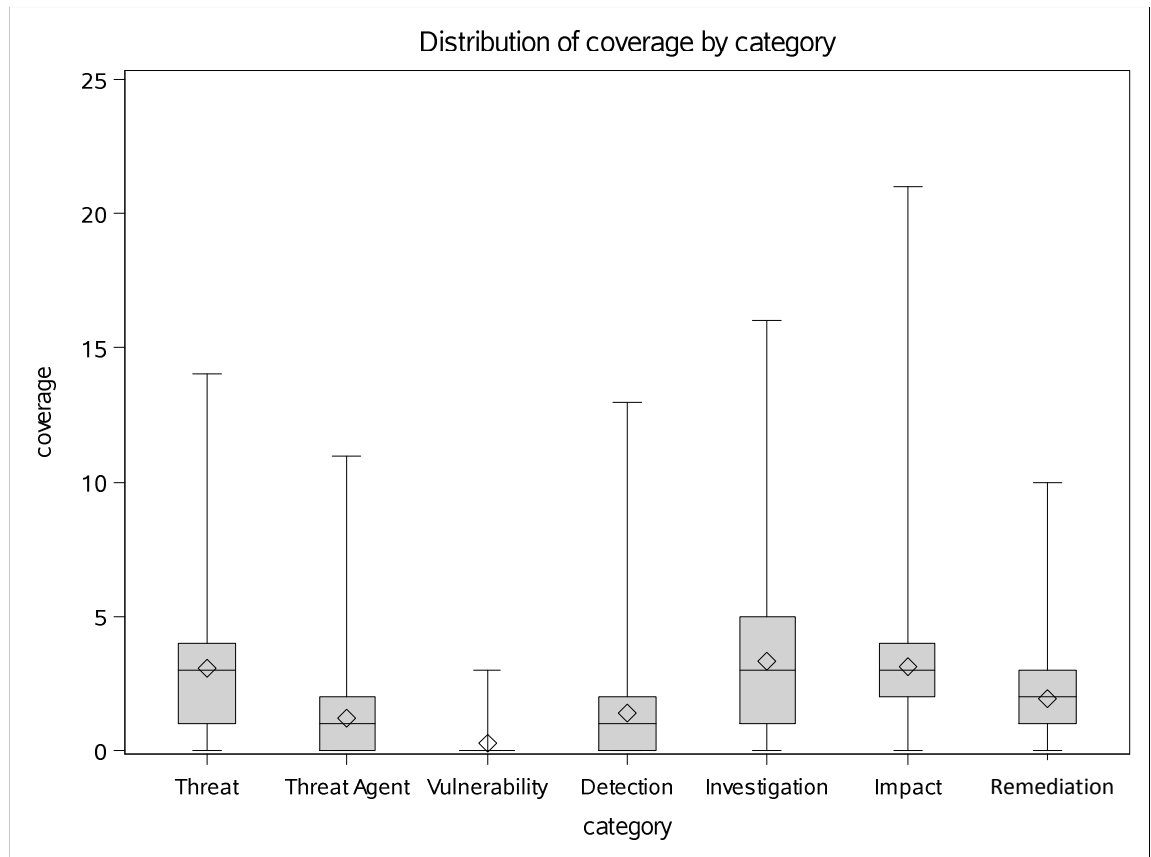


Figure 5-6 Disclosure Coverage of Common Elements

Disclosure reports may also contain multiple sentences that describe a particular element in great detail. The result shows that in terms of investigation and impact, the maximum sentence count is as high as 16 and 21; indicating that the reporting organization has

exerted a considerable effort in providing information on that particular element. On average, organizations spent more effort in describing the threats (3.07), investigations (3.3), and impacts (3.16); but with respect to vulnerability, organizations are less forthcoming with information.

5.6.1 Ambiguous disclosure

If no sentence in a disclosure were found to describe any of the seven elements, it would be considered “*ambiguous*” as no information is provided to describe that particular aspect. Table 5-5 shows the percentage of ambiguous disclosure elements separated by industry in each of the disclosure elements. From the table, the evidence shows that the communications (50%), financial (67%), and insurance (57%) industries have the highest percentage of ambiguous disclosure in terms of threat agent, which means that the majority of the disclosures in these industries failed to identify who or what was responsible for the security breach. Examining the descriptive statistics further in terms of the elements of disclosure, it is also alarming that while most disclosures describe the threat (nature of the event, 14% incomplete) and investigations (9% incomplete) well, a great majority of disclosure (74%) fail to describe the vulnerabilities (What weaknesses were exploited that led to the security breach).

Overall, among the 859 samples, only 26% of the disclosure reports have at least one sentence that discussed vulnerability. Upon further investigation, it is worth noting that the financial industry, despite breach disclosures are also required by GLBA, have an overall high percentage of ambiguous disclosure, even though the word counts (715.62)

and sentence counts (38.12) are well above average (646.64 and 34.31). This suggests that while the disclosure itself might be long, length of disclosure does not necessary translate to information content.

Table 5-5: Percentage of Ambiguous Reporting

<i>Industry</i>	<i>Reports</i>	Threat Agent		Threat		Vulnerability		Detection		Investigation		Remediation	
		<i>Ambi- guous</i>	<i>%</i>	<i>Ambi- guous</i>	<i>%</i>	<i>Ambi- guous</i>	<i>%</i>	<i>Ambi- guous</i>	<i>%</i>	<i>Ambi- guous</i>	<i>%</i>	<i>Ambi- guous</i>	<i>%</i>
IT	29	7	24%	4	14%	16	55%	8	28%	1	3%	2	7%
Communication	4	2	50%	1	25%	4	100%	2	50%	0	0%	1	25%
E-Commerce	27	12	44%	3	11%	17	63%	10	37%	4	15%	5	19%
Education	42	18	43%	4	10%	27	64%	14	33%	0	0%	3	7%
Financial	192	128	67%	14	7%	168	88%	31	16%	37	19%	19	10%
Hospitality	76	31	41%	24	32%	58	76%	30	39%	6	8%	24	32%
Insurance	21	12	57%	1	5%	19	90%	9	43%	6	29%	7	33%
Manufacturing	31	9	29%	4	13%	22	71%	9	29%	6	19%	3	10%
Medical	165	59	36%	25	15%	125	76%	54	33%	7	4%	42	25%
Others	39	10	26%	5	13%	20	51%	9	23%	1	3%	8	21%
Public	27	14	52%	5	19%	25	93%	11	41%	1	4%	9	33%
Retail	71	19	27%	10	14%	50	70%	16	23%	5	7%	6	8%
Service	135	50	37%	13	10%	86	64%	40	30%	11	8%	15	11%
<i>All Industries</i>	859		41%		14%		74%		33%		9%		19%

5.7 Summary

This chapter focuses on the extraction of information content from unstructured breach disclosure reports. Using a novel approach that combines the strength of human processing (GTM) and computerized textual analysis, specialized lexicon and extraction rules using common elements were defined through GTM, followed by the employment of textual analysis techniques to extract evidence of compliance programmatically. The result is an efficient and reliable way to extract information content from disclosure reports consistently. After extraction, the information contents were coded into an accompanying XML document to be used for further analysis. Results of the extractions show several alarming findings of current disclosure practices.

- The annual number of disclosure reports has been increasing since 2012, however, average reporting delays have increased quite significantly year after year. In 2012, the average reporting delay was 80 days; in 2015, the delay has further eroded to 201 days.
- 41% of disclosures are from the medical (19%) and financial (22%) industry (Table 5-3); however, this does not necessary mean that the financial and medical sector suffer more security breaches as there are existing requirements for the financial (GLBA) and the medical (HIPAA) industry. This could be evidence that organizations in other industries are not forthcoming in disclosure.
- Breached organizations are more eager to describe threat agents and threats but are less likely to review their vulnerabilities (Table 5-4). This implies that

organizations are more eager to allocate the blame instead of reviewing what weakness lead to the breach. To improve disclosure practices in the future, more effort on describing vulnerabilities might be needed.

- The financial sector, even though there are existing disclosure regulations in place, performed poorly in terms of providing details in their disclosure reports as shown in Table 5-5. Even though the reports provided by the financial sectors are generally longer in terms of both word counts (715.62 words, average: 646.64, Table 5-3) and sentence counts (38.12 sentences; average: 34.31, Table 5-3), the coverage in terms of providing details in each of the seven common elements is lacking. In addition, the financial industry also has the longest average reporting delays than any other industries (275.8 days; average: 149.67, Table 5-3). However, the medical industry, also governed by a federal regulation, does not show similar lapses.

6 Evaluating Security Breach Disclosure (RQ3)

6.1 Quality Domains & Measuring Instruments of Disclosure

Economic theories inform us that management exerts controls in the accuracy, timing, and content of disclosure (see review in Chapter 2). Therefore, the information content for each of the disclosure elements may have degrees in their properties that are above and beyond the dichotomous demarcation of “disclosed or not-disclosed.” For example, an organization may disclose information regarding what happened (the nature of the breach) but provided very little detail about it. An organization may also selectively disclose or emphasize certain elements of the breach, such that the deficiencies in one area of disclosure could be masked by flooding excess information into other areas. Whether the information is provided fully or partially in all seven elements would indicate the “completeness” aspect of the disclosure. However, completeness of information could only be useful if the information is provided in a timely manner. Time references for specific events about the breach provide timing information which is a key determinant of useful and relevant information in order to improve efficient decision making (O'Reilly, 1982).

Due to variations in accuracy, timing, and content, the quality and the decision usefulness of the disclosure report may vary greatly. Quality is, to some extent, a difficult concept to define since the term “quality” implies usefulness to the user of the information. To

measure quality, there must exist a commonly agreed benchmark so that each subject can be evaluated with a consistent instrument to ensure the reliability of the measure. Since the academic community has not reached a consensus on the definition of quality, prior research has concentrated on factors such as ambiguity (Humpherys et al., 2011), readability (Gunning, 1969), and information richness (Botosan, 1997, Botosan & Plumlee, 2002) as proxy measures of quality disclosure. In addition, various other proxy measures for quality have also been utilized - for instance, vividness and the use of graphics (Lurie & Mason, 2007), or the use of sentiment analysis on the “tone” of corporate annual financial disclosures (Amernic et al., 2010).

Studies in the accounting discipline have introduced many potential quality measure that could be adopted; however, there is no commonly acceptable benchmark to evaluate the quality of security breach disclosure. Without the presence of a standard benchmark, it would be difficult to discern what is a “good” or a “high-quality” disclosure. For instance, the involvement of law enforcement may result in delays of disclosure; on the other hand, having external, impartial parties involved in the investigation process would likely enhance the quality of the disclosure through added credibility. Therefore, a single quality measure is unlikely to determine the quality aspect of each particular element of disclosure. Rather, it is management’s effort to provide the necessary detail to the reader that would likely be most relevant to the affected party. Generally speaking, the objective of disclosing information to stakeholders is to help the different parties in the decision making process to perform certain actions. If a disclosure cannot be delivered to a relevant party in a timely manner or the information content itself contains little or no

information about the timing of related events, or the information contained in the disclosure are missing important details, it may be said that the disclosure is of low quality since it matters little to the intended stakeholder audience.

Another important aspect of disclosure quality is the level of management involvement, which is an additional dimension of completeness measure. This allows the study to gauge the disclosure not only on whether information on a particular element is provided, but also on the richness of the information presented. In addition to the usefulness of breach disclosure to decisions by external stakeholders, the quality of breach disclosure may also have significant impacts on the organization. For example, the lack of quality or detail in the breach disclosure may draw more attention to the organization and increase perceived uncertainties in its operations and quality of its products (Akerlof, 1978). The quality of breach disclosure can also be affected by the quantity of information presented to users. This is particularly the case when the disclosure is signed by the CEO or executive management of publicly traded organizations. The quantity of information to be released in this case is carefully considered before it is made available externally, since such information is usually followed by market analysts.

To summarize, the value and the decision usefulness of any security breach disclosure are related to the timeliness of decision-relevant information, the completeness and richness of detail, and the level of management involvement in the process. The following section discusses the measurement aspect of these three factors.

6.2 Methodology

6.2.1 Measuring Completeness

Chapter 4 established the common elements of breach disclosure, which contains the information about *threat agents*, *threats*, *vulnerability*, *discovery* of the incident, *investigation*, potential *impact*, and *remediation* actions. These elements provide the baseline information of the security breach to the stakeholders. Whether the information is provided fully in all seven elements or only partially indicates the “completeness” aspect of the disclosure.

6.2.2 Measuring Time References and Timeliness of Disclosure

“Timeliness means having information available to decision-makers in time to be capable of influencing their decisions. Generally, the older the information is the less useful it is.” (IASB, 2010). To operationalize the concept in academic research, timeliness, or “disclosure delay” can be defined as days from the date of the fiscal quarter or year-end date to the date of official financial disclosure. However, in terms of security breach disclosure, the concept of timeliness can be quite nuanced as it could encompass multiple measures of timeliness. This is because security breach disclosure is not a periodic event with a definitive, pre-scheduled time to disclose; in addition, there are multiple points in the event life cycle of a security breach that could potentially serve as reference points for timeliness issues on security breach disclosures. Figure 6-1 illustrates the potential measures of timeliness for security breach disclosure.

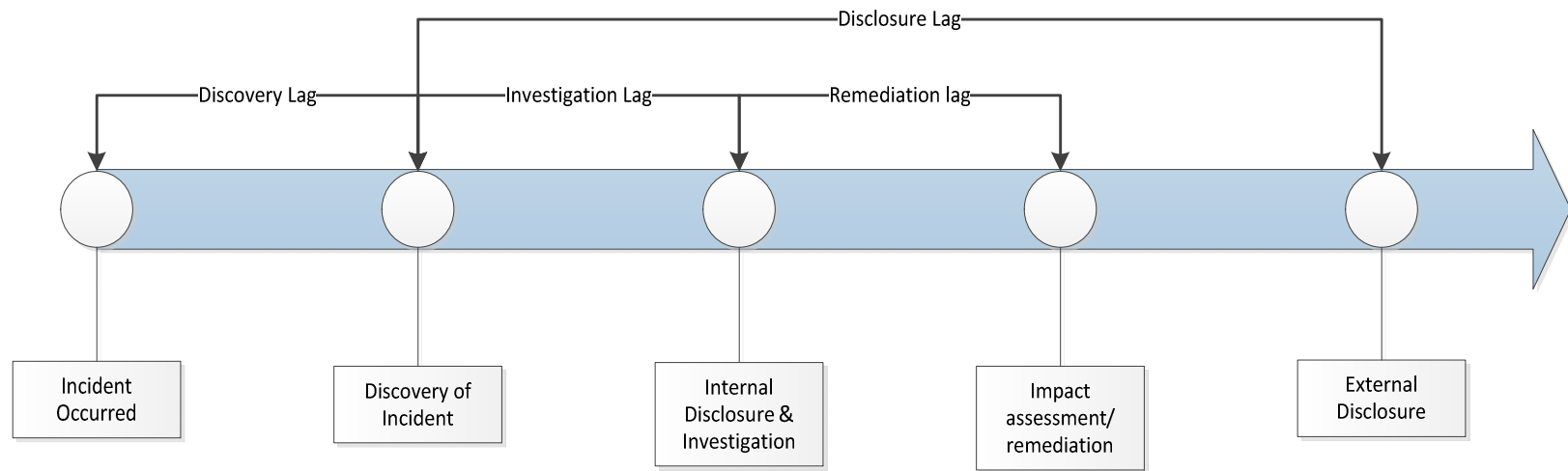


Figure 6-1: Timeliness Issues for Security Breach Disclosure

Discovery lag is the lag time between the actual occurrence of the security incident and its discovery. The disclosure of both the incident date and the discovery date is important as it allows the user of the breach disclosure to determine the organization's information security management capability in detecting the attack. If the incident date is not given (or not known), it casts reasonable doubts over the organization's ability to determine how long the attackers have been accessing the system or how long has the breached data has been in the hands of the attackers. The longer the discovery lag the greater the level of uncertainty in the organization's ISM (Information Security Management) capability.

Investigation lag is defined as the lag time between the discovery of the incident and the beginning of the internal or external investigation. Immediately upon the discovery of the security incident, an active ISM system should activate incident response management processes through internal reporting of the incident. At this point, the incident response management processes should inform the personnel responsible for investigation, and begin other incident response management processes. A significant lag between the incident discovery to the start of the investigation signals the organization's inability or inexperience in dealing with security incidents. It also indicates that there might be a flaw in the internal reporting processes such that management was not informed or ill-informed of the incident.

Remediation lag is defined as the lag time between the start of investigation and the time remediation actions were taken. An adequate investigation of the security incident and proper risk management procedures is required in order to understand the extent and

potential impact of the security breach. Without a proper investigation and impact assessment, the remediation effort could be inadequate as it might be undertaken without a complete picture of the breach. Therefore, a remediation lag could potentially signal that the organization may not have a written incident response procedure that outlines the responsibilities of the investigation and impact analysis effort. It may also reflect the organization's inability to take remediating action in time to address the security incident adequately.

Disclosure lag is defined as the lag time between the discovery of the security incident to the date of external disclosure. This measure is the most common measure for timeliness of disclosure and is used by most regulators. For example, the new GDPR from the EU requires organizations to submit an initial disclosure to the regulator within 72 hours of the discovery of the security incident while other regulators, such as US and Canada, do not have a strict disclosure lag requirement. Disclosure lag is important to the information receiver as a breach of personal data usually requires timely remediation to prevent further damage. If the lag is too long, the breached personal information might be used to execute more attacks. On the other hand, the disclosure lag also serves as a general indicator of the ISM capabilities of the breached organization. If an organization takes too long to disclose a breach, it might signal that its incident management processes are flawed.

Ideally, a disclosure timeliness measuring instrument should yield all measures of timeliness since it reflects different aspects of the organization's ISM capabilities and its

ability to determine the exact timing of events that occurred. However, based on the sample data obtained in this study, current practices in providing a detailed timing of events are severely lacking. On average, references to timing of events are provided sporadically (Table 6-5). In the financial sector, on average the references to time are 0.75, meaning that 25% of the reports have no timing references in them at all. In these cases it would be impossible for the stakeholder to determine when the breach occurred. To overcome the deficiency due to lack of disclosure on timing of events, an alternative measure – time reference could be used, which measures how many times a specific date has been identified in a report. This alternative proxy measure, although imperfect, is a reasonable proxy as it reflects the organization's ability and willingness to provide timing details to stakeholders. Table 6-1 presents a sample report with detailed time references. This particular report provided 16 time references in describing the breach event.

Table 6-1 Example of a Detailed Report with Multiple Time References

<p>1. August 13, 2012: A malicious (phishing) email was sent to multiple Department of Revenue employees. At least one Department of Revenue user clicked on the embedded link, unwittingly executed malware, and became compromised. The malware likely stole the user's username and password. This theory is based on other facts discovered during the investigation; however, Mandiant was unable to conclusively determine if this is how the user's credentials were obtained by the attacker.</p> <p>2. August 27, 2012: The attacker logged into the remote access service (Citrix) using legitimate Department of Revenue user credentials. The credentials used belonged to one of the users who had received and opened the malicious email on August 13, 2012. The attacker used the Citrix portal to log into the user's workstation and then leveraged the user's access rights to access other Department of Revenue systems and databases with the user's credentials.</p> <p>3. August 29, 2012: The attacker executed utilities designed to obtain user account passwords on six servers.</p> <p>4. September 1, 2012: The attacker executed a utility to obtain user account passwords for all Windows user accounts. The attacker also installed malicious software ("backdoor") on one server.</p> <p>5. September 2, 2012: The attacker interacted with twenty one servers using a compromised account and performed reconnaissance activities. The attacker also authenticated to a web server that handled payment maintenance information for the Department of Revenue, but was not able to accomplish anything malicious.</p> <p>6. September 3, 2012: The attacker interacted with eight servers using a compromised account and performed reconnaissance activities. The attacker again authenticated to a web server that handled payment maintenance information for the Department of Revenue, but was not able to accomplish anything malicious.</p> <p>7. September 4, 2012: The attacker interacted with six systems using a compromised account and performed reconnaissance activities.</p> <p>8. September 5 - 10, 2012: No evidence of attacker activity was identified.</p> <p>9. September 11, 2012: The attacker interacted with three systems using a compromised account and performed reconnaissance activities.</p> <p>10. September 12, 2012: The attacker copied database backup files to a staging directory.</p> <p>11. September 13 and 14, 2012: The attacker compressed the database backup files into fourteen (of the fifteen total) encrypted 7-zip1 archives. The attacker then moved the 7-zip archives from the database server to another server and sent the data to a system on the Internet. The attacker then deleted the backup files and 7-zip archives.</p> <p>12. September 15, 2012: The attacker interacted with ten systems using a compromised account and performed reconnaissance activities.</p> <p>13. September 16, 2012 – October 16, 2012: No evidence of attacker activity was identified.</p> <p>14. October 17, 2012: The attacker checked connectivity to a server using the backdoor previously installed on September 1, 2012. No evidence of additional activity was discovered.</p> <p>15. October 19 and 20, 2012: The Department of Revenue executed remediation activities based on short term recommendations provided by Mandiant. The intent of the remediation activities was to remove the attacker's access to the environment and detect a recompile.</p> <p>16. October 21, 2012 – Present: No evidence of related malicious activity post-remediation has been discovered.</p>
--

6.2.3 Measuring Management Involvement

Management involvement is among the most important factors in ensuring the success of ISM (Von Solms & Von Solms; 2004). In terms of security breach disclosure, higher

level management's involvement could potentially enhance the credibility and trustworthiness of the report. Credibility, according to Merriam-Webster dictionary, is defined as *“the quality or power of inspiring belief and trust.”* This is an important quality aspect of disclosure as the disclosures may be complete and rich in terms of the information content; however, if there is little evidence of management involvement (for example, lack of executive signatures on the report), the information provided could be of little trustworthiness or unable to inspire belief, thereby being relatively useless to the decision maker. The measurement of credibility has an established research stream in the study of journalism. Gaziano and McGrath (1986) used a factor analysis of 16 items measuring people's attitudes towards newspaper reports to show that credibility is highly associated with accuracy, trustworthiness, and whether the reports “tell the whole story”. These dimensions translate to the use of reference checking, editorial (management) oversights, and third party validations. To measure management involvement in self-reported breach disclosure, this study uses the following measures to help determine the level of management involvement:

- Whether law enforcement authorities were involved in the investigation process
- Whether specialists, such as forensic accountants or external security consultants were involved in the processes.
- Whether senior management were involved in the disclosure.
- Whether the disclosures were signed.
- Whether contact information was provided for reference.

Table 6-2 presents an 87-word disclosure report with little evidence of management involvement. Since it appears that it could have been written by a clerk without any management involvement it inspires little trust.

Table 6-2 Example of Disclosure with Little Management Oversight (StumbleUpon, Inc., SB-44746)

Name	StumbleUpon Inc.
ID	SB-44746
content	<p>StumbleUpon</p> <p>Hi [name],</p> <p>Recently, we detected suspicious activity on your StumbleUpon account. To keep you safe we have locked your account and reset your password.</p> <p>To regain access, you will need to confirm your username ([name]) and email address here.</p> <p>How can this happen? People often use the same password across multiple services, which can put you at risk. To minimize your exposure, StumbleUpon recommends using A unique passwords for each service that you use.</p> <p>Thanks for your cooperation as we seek to restore your account,</p> <p>Team StumbleUpon</p>

6.2.4 Scoring with Point Systems

In Chapter 5 – Extraction of Information Content, each sentence is the base unit of analysis. Under this rule, a single sentence containing multiple elements of disclosure, could satisfy as evidence for compliancy. On the other hand, if multiple sentences are used to describe any of the seven major elements, the added score would represent the information richness aspect of the particular element. For example, Table 6-3 shows how threat agent identification is evaluated.

In this example, SB24-22211 contains 3 sentences describing the nature of the threat agent while SB24-22123 uses only one sentence. The accumulated score would be 3 under threat agent identification for SB24-22211 and 1 under threat agent identification for SB24-22123. Following Botosan's (1997) work on measuring the level of disclosure in financial annual reports, in this study I adopt its method of using a simple point system that awards each item of evidence a point score. In an ideal setting a factor analysis should be performed to determine the weight of each element; however, in the absence of a commonly agreed benchmark, it is impossible to determine which element would be awarded the higher weight. In addition, the system does not evaluate how well a sentence is written in terms of its use of language or readability (Kincaid et al., 1975). Because security breach reports could contain technical terms that are not commonly used, the readability aspect of disclosure reports might not be as important as other factors.

Table 6-3: Threat Agent Identification – External Agents

ID	Task	Context	Score	Evidence
sb24-22123	Threat Agent Identification	external	1	On the night of December 29, 2011, a laptop used in preparation for the merger of SF Fire Credit Union with Pacifica-Coastside Credit Union was stolen from a parked car in San Francisco.
sb24-22211	Threat Agent Identification	external	1	An illegal and unauthorized intrusion regrettably occurred, which may have caused your personal information to be compromised.
sb24-22211	Threat Agent Identification	external	1	We recently became aware of a criminal intrusion into our ActiveStore Web-based storefront application that processes purchases of digital games made by customers on our partners' Web sites.
sb24-22211	Threat Agent Identification	external	1	We believe the intruders may have been able to intercept and obtain cardholder names, credit card account numbers, expiration dates, security codes, postal addresses, email addresses, and passwords to optional user accounts on ActiveStore storefronts from a portion of transactions flowing through the ActiveStore application between November 4, 2011, and December 2, 2011.
sb24-22302	Threat Agent Identification	external	1	If you have accessed your Steam account since November 10, 2011 you know that we had a network intrusion.
sb24-22302	Threat Agent Identification	external	1	We learned about this intrusion when the Steam forums were defaced on November 6. Since then our investigation of this intrusion has continued with the help of outside security experts.
sb24-22302	Threat Agent Identification	external	1	We've recently learned that it is probable that in 2009 the intruders obtained a copy of a database with information about Steam transactions between 2004 and 2008.
sb24-22311	Threat Agent Identification	external	1	On December 31, 2011, a thief(ves) broke into our office.
sb24-22311	Threat Agent Identification	external	1	The thief(ves) broke into a locked area of the office and stole a number of items, including computer hardware that was used to back-up some of our computer systems.
sb24-22542	Threat Agent Identification	external	1	Regrettably, on February 6, we were notified that a desktop computer was stolen from the office of The Renaissance Group, LLC.
sb24-22725	Threat Agent Identification	external	1	A BDO employee removed the CD-ROM from site, where they believe it was stolen from her vehicle.
sb24-22725	Threat Agent Identification	external	1	Rubio's understands your name was included on the CD-ROM which was stolen.
sb24-22725	Threat Agent Identification	external	1	A BDO employee accidentally removed the CD-ROM from site, where it may have been stolen from her vehicle.

6.3 Evaluation Results

Table 6-4 represents the composite index score for completeness, time references and management involvement from the 859 California disclosure reports evaluated using the point system. The maximum score of any report for time references is 19, which indicates that the particular report disclosed 19 separate instances mentioning timing of a particular event, procedure, or steps that took place.

Table 6-4 Composite Scores of Completeness, Time References, and Management Involvement

<i>Composite indexes</i>	<i>Maximum</i>	<i>Mean</i>	<i>Median</i>	<i>Minimum</i>	<i>Std Dev</i>
Completeness score	7	4.93	5	0	1.32
Time References score	19	1.66	2	0	1.51
Management Involvement score	5	2.73	3	0	1.2
Total score	27	9.33	9	0	2.67

Table 6-5 presents the average completeness, time references, and management involvement score each year since 2012. Using a simple linear regression on the observations from 2012 to 2016 that test the slope, the evidence shows both completeness and management involvement are statistical significant (completeness, t-value: 2.21; management involvement, t-value: 1.84) and positive coefficient (completeness, coefficient: 0.215; management involvement: 0.155). It can thus be inferred that completeness and management involvement are improving over the year. Although the sampled years only cover reports from 2015 to 2016; it could be an early indication that

disclosures have improved gradually. Figure 6-2 and 6-3 depicts the fit plot for the completeness and management involvement from the complete sample.

Table 6-5 Composite Score by Year

<i>Year</i>	<i>Reports</i>	<i>Completeness</i>	<i>Time References</i>	<i>Management Involvement</i>	<i>Total score</i>
2012	126	4.64	1.74	2.83	9.21
2013	161	4.44	1.37	2.42	8.93
2014	179	4.89	1.58	2.78	9.25
2015	202	4.73	1.77	2.91	9.02
2016	189	5.57	1.92	3.36	10.15

Investigating further, Table 6-6 presents the composite score by industry. It is surprising to see that while the financial sector may have the highest number of disclosures due to GLBA requirements, the quality of these disclosures was low. Both completeness (2.74) and time references (0.75) are far below average for all disclosures (4.76 and 1.60).

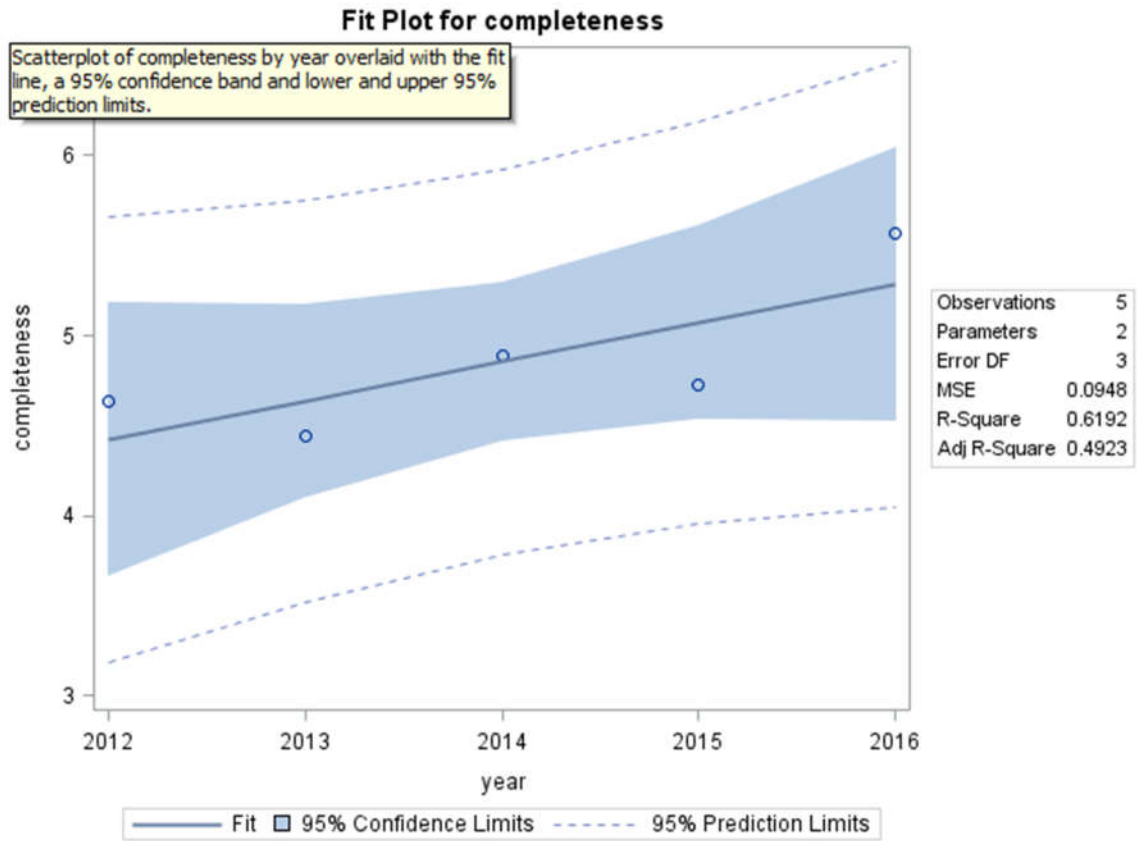


Figure 6-2: Fit Plot for Report Completeness in Security Disclosure from 2012 to 2016

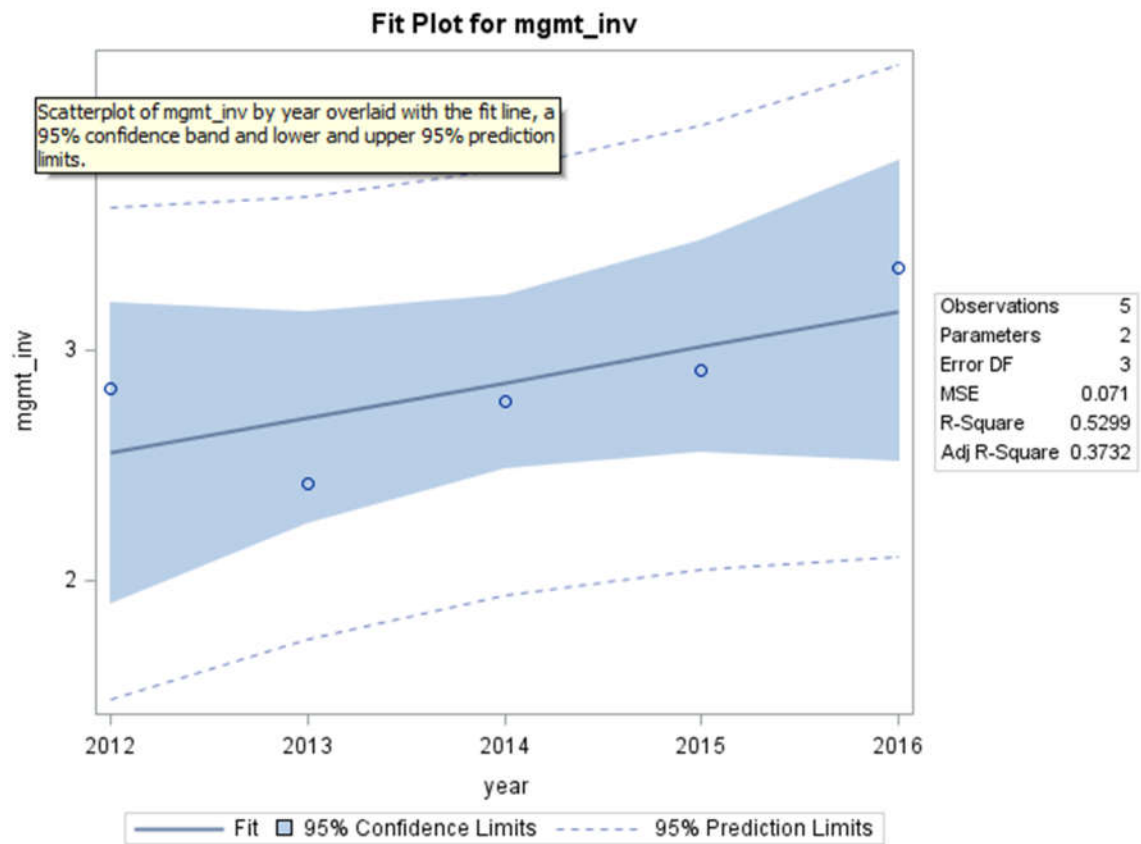


Figure 6-3: Fit Plot for Management Involvement (mgmt_inv) in Security Disclosure
from 2012 to 2016

Investigating further, Table 6-6 presents the composite score by industry. It is surprising to see that while the financial sector may have the highest number of disclosures due to GLBA requirements, the quality of these disclosures was low. Both completeness (2.74) and time references (0.75) are far below average for all disclosures (4.76 and 1.60).

Table 6-6 Composite Score by Industry

<i>Industry</i>	<i>Reports</i>	<i>Completeness</i>	<i>Time References</i>	<i>Management Involvement</i>	<i>Total score</i>
Education	7	5.00	1.29	3.71	10.00
IT	29	5.17	1.25	2.33	8.75
Communication	4	4.75	0.50	2.50	7.75
E-Commerce	27	4.96	1.15	2.70	8.81
Education	35	5.46	1.91	2.71	10.09
Financial	192	2.74	0.75	2.01	8.51
Hospitality	76	4.26	2.20	2.70	9.15
Insurance	21	4.57	1.48	3.05	9.10
Manufacturing	31	5.19	1.68	2.77	9.65
Medical	165	4.72	1.93	3.50	9.14
Others	39	5.17	1.60	2.90	9.67
Public	27	4.19	2.44	1.93	8.56
Retail	71	5.16	2.38	2.98	10.52
Service	135	5.34	1.87	2.81	10.03
All	859	4.76	1.60	2.76	9.27

6.4 Analysis

Using the raw scores obtained from each of the seven elements, table 6-7 presents the Pearson / Spearman correlation table to show variable correlations. From these results, it

appears that report delay (disclosure lag) is positively correlated with detection score, investigation score, third-party involvement, management signature, c-level (CEO, CFO, CIO, or CSO) or senior management involvement. This suggests that when more details of detection and investigation are provided, the disclosure is more likely to have a longer reporting delay.

Table 6-7 Evaluation Score Pearson / Spearman Correlation

Variable	Report Delay	Agent Int Score	Agent Ext Score	Threat Score	Vuln. Score	Detecti on Score	Investi- Gate Score	Impact Score	Remed iation Score	Date Full Score	Apology Score	Third- Party Score	Signed Score	Clevel Score
Report Delay		-0.051	-0.030	-0.011	-0.009	0.195	0.091	-0.058	-0.018	-0.133	-0.152	0.118	0.035	0.052
Agent Int Score	-0.051		-0.095	0.009	0.057	-0.063	-0.134	0.005	0.070	0.058	0.120	-0.139	0.030	-0.051
Agent Ext Score	-0.030	-0.095		0.182	0.133	0.046	0.206	0.315	0.160	0.241	0.110	0.173	-0.029	-0.037
Threat Score	-0.011	0.009	0.182		0.059	0.085	0.434	0.518	0.333	0.146	0.071	0.415	0.017	-0.021
Vulnerability Score	-0.009	0.057	0.133	0.059		0.000	0.083	0.048	0.105	0.199	0.022	0.031	-0.091	-0.071
Detection Score	0.195	-0.063	0.046	0.085	0.000		0.093	0.077	0.110	-0.032	-0.195	0.094	-0.118	-0.032
Investigate Score	0.091	-0.134	0.206	0.434	0.083	0.093		0.406	0.418	0.115	0.016	0.867	0.147	0.176
Impact Score	-0.058	0.005	0.315	0.518	0.048	0.077	0.406		0.324	0.215	0.149	0.366	0.056	0.042
Remediation Score	-0.018	0.070	0.160	0.333	0.105	0.110	0.418	0.324		0.215	0.133	0.361	0.119	0.157
Date Full Score	-0.133	0.058	0.241	0.146	0.199	-0.032	0.115	0.215	0.215		0.201	0.016	0.039	-0.089
Apology Score	-0.152	0.120	0.110	0.071	0.022	-0.195	0.016	0.149	0.133	0.201		-0.052	0.048	-0.034
Third-Party Score	0.118	-0.139	0.173	0.415	0.031	0.094	0.867	0.366	0.361	0.016	-0.052		0.123	0.179
Signed Score	0.035	0.030	-0.029	0.017	-0.091	-0.118	0.147	0.056	0.119	0.039	0.048	0.123		0.672
Clevel Score	0.052	-0.051	-0.037	-0.021	-0.071	-0.032	0.176	0.042	0.157	-0.089	-0.034	0.179	0.672	

It is interesting to note that if disclosure is signed by a member of management or c-level upper management, the correlation with report delay is positive. This suggests that these management officials are likely to take more time, requiring more careful consideration of facts about the data breach, before personally signing the disclosure.

In terms of threat agents, I separate internal threat agents and external threat agents for comparison. Based on these differences it appears that for internal threat agents there is less effort given to detection, investigation, and third party involvement in the disclosure; on the other hand, breaches that involve external threat agents show positive correlations with detection, investigation, and third party involvement. This clearly shows that disclosures are handled differently if threat agents are internal employees. Explanations for such differences will require more in-depth study in the future.

6.5 Factors that Affect Disclosure Scores

To provide a further analysis of what aspects of breach disclosure would affect completeness, time references, and management involvement scores, I used generalized least squares model (GLM) to facilitate the multivariate statistical analyses. The dependent variables are the completeness, time references, management involvement, and the composite score of the disclosure. The independent variables are the raw scores of the descriptions in each of the seven elements. In addition to the raw scores, additional variables and the meta properties were included to provide additional insights to what factors might affect the quality of the disclosure. Table 6-8 presents the variable descriptions.

Table 6-8 Variable Description

Variable	Description
<i>Threat Agent Sscore</i>	The raw score of description in threat agent
<i>Threat Score</i>	The raw score of description in threat
<i>Vulnerability Score</i>	The raw score of description in vulnerability
<i>Detection Score</i>	The raw score of description in how events were discovered
<i>Investigate Score</i>	The raw score in describing the investigative efforts
<i>Impact Score</i>	The raw score in describing the impact and impact analyses.
<i>Remediation Score</i>	The raw score of description in the remediation effort.
<i>Apology Score</i>	If any form of apology is offered in the customer disclosure
<i>Third-party Score</i>	If any third party involvement is disclosed
<i>Signed Score</i>	If the disclosure is signed
<i>C-level Involvement</i>	If any C-level senior management level executives are involved
<i>Internal Breach</i>	If the breach is caused by internal sources
<i>External Breach</i>	If the breach is caused by external sources
<i>Sentence Count</i>	How many sentences are in the disclosure
<i>Word Count</i>	The raw word-counts of the disclosure
<i>Report Delay</i>	The disclosure delay

To ensure multicollinearity does not reduce the predictive power or reliability within the sample data set, I checked the correlation table of all variables used. There were no correlations above 0.75, indicating that overfitting should not be a problem in the model.

To account for the potential differences in disclosure practices in years and in different industry, year-fixed effects and industry-fixed effects are considered in the GLM model so that the effects of the independent variables on the scores are free from the influences of any particular year or particular industry.

Generalized Least Squares Model:

Table 6-9 presents the results of the GLM model. The results for completeness, time references, management involvement and the composite score are presented in column (1), (2), (3), and (4). The results reveal several interesting statistical inferences:

Completeness Rating:

- Vulnerability description has a high impact on the completeness score. This is logical as very few disclosures provided vulnerability descriptions.
- C-level management involvement has a positive and significant effect on the completeness rating.
- If the breach reports clearly identify whether the breaches are from either internal or external sources, the existence of such disclosures are highly associated with the completeness rating of the disclosure. This suggests that if an organization has disclosed the sources of the attack, there is a high likelihood that other elements of disclosure would also be adequately disclosed.
- Sentence counts, surprisingly, have a significant and negative effect on completeness. This suggests that longer reports do not necessarily make the information content more complete. In addition, word count also shows that there is very little (0.0007) association between word counts and the completeness of the report. This is an important finding as the result also shows that high quality ratings are not attributed to wordy, long reports.

- The report delay estimate shows that the delay does not necessarily make the report more or less complete as the coefficient estimate is small and statistically insignificant. This finding would invalidate the argument that longer times taken to prepare reports would make disclosures better.

Time References Ratings:

- The time references rating is highly associated with the description of threat agent, vulnerability, and remediation. Event time is usually mentioned in an organization's effort to describe "what has happened"; therefore, it is logical to find this positive association. On the other hand, an organization's remediation effort usually comes in the form of free credit monitoring service with an expiration date. Therefore, it is also logical to draw the inference that time references ratings are associated with organizations' effort in describing remediation solutions.
- It is surprising to find that there are few evidence of detection in the time references rating. This suggests that the disclosure of when incidents were detected is lacking in the current sample.
- Third party involvement has a negative and significant association with the time references rating of the disclosure. This suggests that the involvement of third parties, while improving overall credibility of the report, may make the reporting organization reports less on the time references due to more delays or involving more effort to state the specific time references more complicated.

- Interestingly, C-level senior management involvement has a negative and statistically significant effect on time references ratings. This suggests that senior management oversight, while improving completeness, does not make time references in the disclosure more accessible. From the correlation analysis, positive correlation between senior management oversight and report delays (in calendar days) were also observed.

Management Involvement Rating

- The results show a significant and negative association between vulnerability, threat, and detection. This suggests that the more effort that is expended into describing the “negative” aspects of the report, the lower the management involvement rating would be. On the other hand, the more effort spent in describing the investigation, impact analysis, and remediation the higher the management involvement rating would be. This suggests that management’s preference towards more attention on solutions and not on the problems that caused the breach.
- Interestingly, the results show a negative association between management involvement and the use of “apology” in the disclosure. This suggests that the literal use of the word “apology” was, most likely, just lip service.

Composite Score:

Overall, the multivariate regression results (Table 6-9) show that descriptions of vulnerability (1.1437), investigation (0.2608), remediation (0.3528), signed disclosure (1.4985), and senior management oversight (0.7532) have positive and statistically significant effects on the overall quality of the disclosure.

Table 6-9 General Least Squares Model with Fixed Effect

	(1)	(2)	(3)	(4)
Dependent Variable	Completeness	Time Reference	Management Involvement	Composite
<i>Parameter</i>	<i>Estimate</i>	<i>Estimate</i>	<i>Estimate</i>	<i>Estimate</i>
<i>Threat Agent Score</i>	-0.0291	0.1436 ***	-0.0030	0.1116 **
<i>Threat Score</i>	0.0878 ***	0.0092	-0.0105 **	0.0865 **
<i>Vulnerability Score</i>	0.7824 ***	0.4908 ***	-0.1295 ***	1.1437 ***
<i>Detection Score</i>	0.1093 ***	0.0404	-0.0388 ***	0.1109 **
<i>Investigate Score</i>	0.1438 ***	0.0827	0.0343 **	0.2608 ***
<i>Impact Score</i>	0.0523 ***	0.0020	0.0243 ***	0.0786 **
<i>Remediation Score</i>	0.1085 ***	0.2001 ***	0.0442 **	0.3528 ***
<i>Apology Score</i>	-0.0224 ***	0.0393	-0.0407	-0.0238
<i>Thirdparty Score</i>	0.0029	-0.1719 ***	0.0908 ***	-0.0782
<i>Signed Score</i>	0.0408	0.3659	1.0918 ***	1.4985 ***
<i>C-Level Involvement</i>	0.1779 **	-0.3478 ***	0.9230 ***	0.7532 ***
<i>Internal Breach</i>	0.8214 ***	-0.1322	0.0207	0.7098 ***
<i>External Breach</i>	0.9618 ***	0.0013	0.1929 ***	1.1561 ***
<i>Sentence Count</i>	-0.1120 ***	-0.0034	0.0009	-0.0745 **
<i>Word Count</i>	0.0007	0.0008 **	0.0004	0.0009
<i>Report Delay</i>	0.0002	-0.0002	-0.0002 **	-0.0004
<i>Industry Fixed Effect</i>	Yes	Yes	Yes	Yes
<i>Year Fixed Effect</i>	Yes	Yes	Yes	Yes
<i>Adjusted R-Square</i>	0.6317	0.6866	0.7365	0.6390

Note: 1. For Variable definition, see Table 6-8. 2. ***, and ** indicate significance levels of .01, .05 respectively (two-tailed). Significance level at 0.10 is not reported.

6.6 Summary

This chapter has investigated RQ3 which focuses on the evaluation of security breach disclosures. The objective was to determine the quality of disclosure reports and the degree of effort provided by the breached organization. I propose three measures as proxies for quality; 1) the completeness of report coverage, 2) the time references of events that occurred as a result of breaches, and 3) management involvement in the incident response process. Using multivariate regression analyses with generalized least squares model, this chapter provided further detailed results on what aspects of breach disclosure would be associated with the disclosure's completeness, time references, and management involvement.

7 Security Breach Disclosure Framework

7.1 Security Breach Disclosure Framework

This chapter focuses on the future of disclosure regulations, practices, and research, with the objective of exploring future research paths using a framework that would map out the inter-relationships and stakeholder roles in security breach disclosure.

The study suggests four main stakeholders, including the regulators, management of the breached organization, the affected parties, and the information security community, as shown in Figure 7-1. The regulators' main interaction with management is to set rules and conditions for the management on what needs to be disclosed to meet the basic requirements; management of the organization needs to provide the evidence of compliance through actions or documentation of what has been done. Management is primarily responsible for furnishing the disclosure, which must be submitted to the regulators; in addition, regulators would monitor and enforce the disclosure rules based on the disclosure submitted. The breach disclosure, given that adequate information is properly included, would provide timely and relevant information to the affected parties.

The regulators' responsibility to the affected parties is to ensure the right to know; however, the information disclosed by the security breach disclosure may be incomplete or the actions taken by the organization may be insufficient; therefore, the affected parties may demand further protection and actions from the regulators such that more compliance

rules would be applied to organizations that experience security breaches. Upon receiving the disclosure, the affected parties may also demand further assurance and actions regarding remediation. The breach disclosure provided by the organization may not contain adequate information; therefore, the information security community would collect feedback and analyze the experience in order to provide recourse and remediation above and beyond what management has or could offer. From the information security community's perspective, its role is to observe and evaluate security breach disclosures so that the information could add new knowledge and intelligence that would enhance the community's ability to provide guidance and best practices to the breached organization and affected parties. In addition it would also generate a knowledge base that would help to combat future security breaches through new technology or new detection, prevention, and corrective controls.

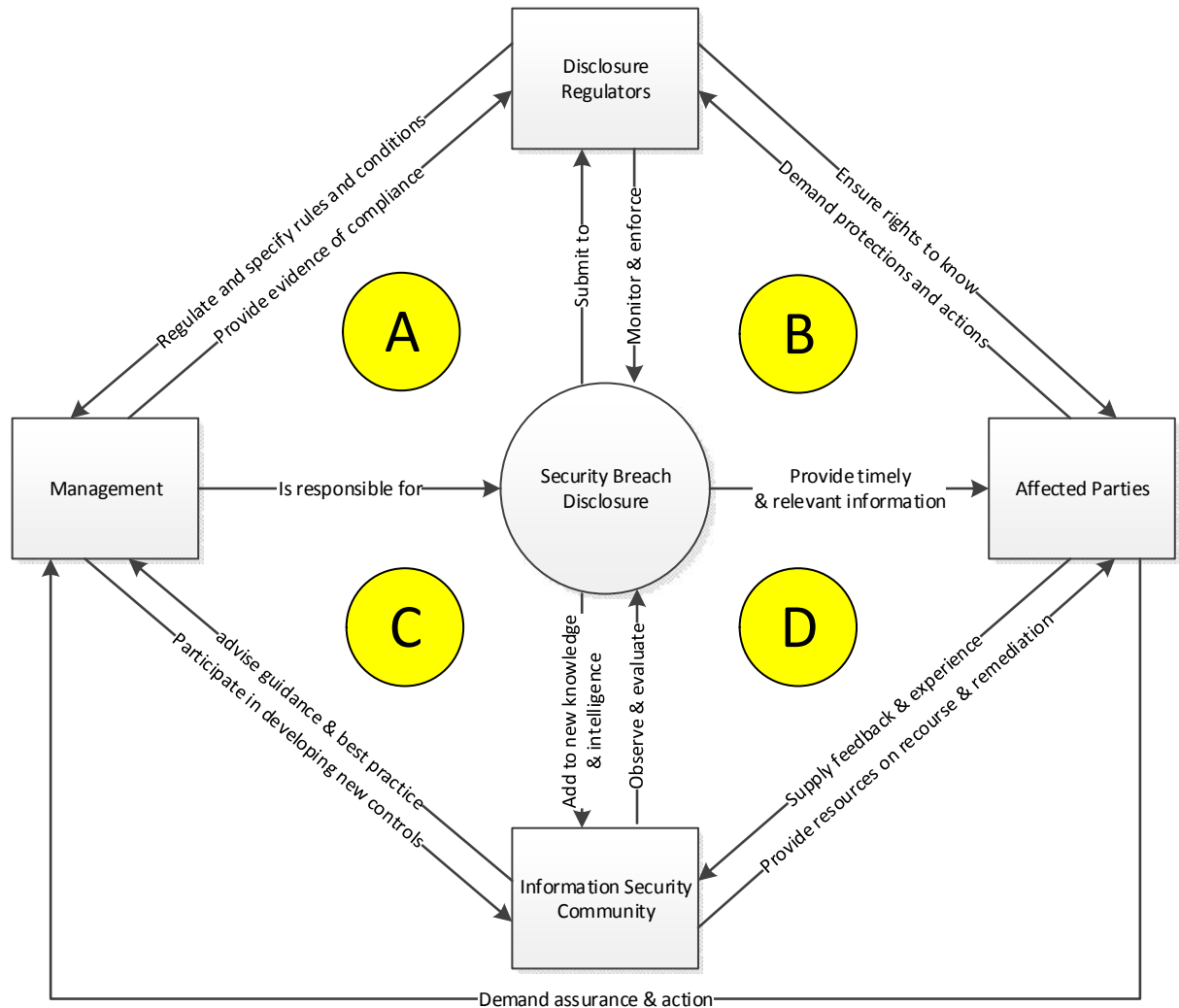


Figure 7-1: Proposed Security Breach Disclosure Framework

7.2 Use of the Framework and Future Research Directions

The framework in Figure 7-1 explains how research can help to understand the relationships of different stakeholders in the disclosure process. The framework depicts 4 main stakeholders and their interactions through security breach disclosure are captured in quadrant A, B, C, and D. Quadrant A represents the interaction through security

breach disclosure between the reporting organization's management and disclosure regulator. Respectively, each quadrant shows the role of management, regulator, affected parties, and information security community in shaping and using security breach disclosure

In this study, RQ1, 2, and 3 explore this interaction in quadrant A, focusing on the interrelationships between the disclosure regulators, management and the disclosure. The study suggests common elements of disclosure requirements so that the rules and conditions of what needs to be disclosed are clear. In RQ2, the study analyzes what is submitted by management such that their work (the information content) can be checked against the responsibility (the regulations). An analysis of the framework shows that there are many areas left unexplored. While analysis of policies and market reactions have shed insights on outcomes of security breach disclosures, these have been but a small portion of studies that could help improve outcomes for affected parties.

7.3 Management Discretion and Disclosure Practices

The framework illuminates the purpose of security breach disclosures to inform interested parties about the threat agents, vulnerabilities, investigations, and remediation efforts surrounding security breaches. However, the framework also shows that more in-depth studies could be undertaken of the interactions of governance, management, and staff on exercising the discretion of control in disclosing breach information. With respect to individual compliance behavior, existing studies show that penalties and sanctions can improve policy compliance efforts. On a larger scale, results from this study show that

the scientific community knows little about compliance behavior on the management or organization level in terms of security breach disclosure.

From the governance perspective, disclosure studies in the financial accounting discipline have explored the association between corporate governance and financial information quality. For instance, Klai and Omri (2011) found that the power of families, foreigners and blockholders tend to decrease the quality of financial statements, but companies facing control from financial institutions or state will produce better quality disclosures. However, in security breach disclosure, very little is known on how governance affects the quality of security breach disclosure. It remains to be seen how independent board oversight affects breach disclosure quality.

7.4 Information Security Community and Knowledge Building for ISM

The framework also shows us that with respect to information security management and knowledge building, the security community as a whole has a significant role. Security breach disclosure allows the community to learn from actual incidents and check evolving threat landscapes against the existing knowledge base. However, what can often be most tenuous and challenging for the community– is not knowing what *we don't know* in a world where threats and threat agents have tools and capabilities to exploit potential vulnerabilities that are either *known are not known*.

National security and intelligence professionals have long used an analysis method referred to as the Johari window technique (Luft & Ingham, 1961), which was famously used by US Secretary of Defense, Donald Rumsfeld,

“There are known- knowns; the things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.”

The Johari analysis technique, particularly, the use of known-known and unknown-unknowns have been used in analyzing risks and uncertainties (Chow & Sarin, 2002). As shown in table 7-1, known-unknowns refer to risks that we are aware of, such as computer virus attacks; Unknown unknowns are risks that come from situations that are outside current knowledge bases and have never occurred. Existing theories for ISM such as Threat Avoidance Theory (Liang & Xue, 2009) could provide knowledge and understanding in the “known-known, known-unknown” quadrant of information security risks. However, the inherent limitations in conventional theory-based security defenses is the requirement of valid “known” observations so to be qualified as a phenomenon. As such, we’re beginning to see limitation as there are simply more threats, agents, and new vulnerabilities that are outside the current knowledge (known-unknown) or outside of the current realm of understanding. (unknown-unknown). Threat agents and new attack vectors can move faster than ever before, mutating malware and actively changing exploiting tactics. Protective security methods are now becoming less useful and unable to fend off new attack vectors, so organizations and the information security community

need to become more proactive in learning from new incidents and new attack vectors.

Breach disclosure plays an important role in enhancing this process.

Table 7-1: Known-unknown Table

	... that we know	...that we don't know
What we know ...	<p>Q1: know-known</p> <p>Explicit knowledge on security risks.</p> <p>Focus: Check against existing control against known threats</p> <p>ISM Techniques: Security checklists, vulnerability scanning</p>	<p>Q2: know-unknown</p> <p>Knowledge GAP on information security risk</p> <p>Focus: Knowledge dissemination from security professionals, new research to bridge knowledge gap.</p> <p>ISM Technique: education, and hiring of security personnel, proactive prevention.</p>
What we don't know	<p>Q3: Unknown-known</p> <p>Tacit knowledge on security practices.</p> <p>Focus: Making tacit knowledge or practice known to organization.</p> <p>ISM Techniques: Awareness training, security culture;</p>	<p>Q4: unknown-unknown</p> <p>No knowledge until discovery</p> <p>Focus: Responsive analysis and data acquisition technique to enable exploration and discovery.</p> <p>ISM Techniques: None</p>

7.5 Summary

Information security risks can never be completely eliminated; in other words, it is not possible to completely prevent adverse security incidents. The study of security breach disclosure introduces an incident-based, data-centric approach in information security knowledge building that can provide practitioners and regulators reliable methods to find previously unobservable patterns in security incidents. These would provide businesses

with actionable intelligence to overcome the knowledge gaps that could otherwise compromise their business.

Ultimately, the goal of information security management is to defend against the unknown threat agents, to proactively prevent new threats, and responsively react to new techniques and events. In this way organization could effectively learn from events that happened within the organization, and accumulate experience to combat threats that are known, and most importantly, enable people, systems, and organizations to learn from each other.

This research encourages effective means to analyze security breach disclosures, which allows individuals, organizations, and policy makers to proactively address knowledge checking, knowledge transfer, knowledge dissemination, and knowledge exploration issues in information security risk management. This can be an effective way to reduce the impact of the unknown.

8 Conclusions

8.1 Discussion of Major Findings

The results from this study reveal many alarming issues in the current regulations and practices of security breach disclosure. These issues and suggestions for potential solutions are summarized in this chapter. The intention of this study is not to provide a silver-bullet solution that would overcome all the challenges. Instead, it aims to raise awareness among regulators, practitioners, and researchers to review the results and to work towards solutions that result in more effective security breach disclosures and their use in helping to combat the flood of security breaches that plague the industrial world. Results for RQ2 (Security information content, and RQ3 (Evaluating security breach disclosure) are based on 859 unique disclosure reports from the California Attorney General during 2012 to 2016. Although these breach disclosure reports do not contain all breach reports in United States; however, it contains the reports that are disclosed by the breach organization and allows this study to investigate the phenomenon across several industries. Although the State of California, like many other regulators, has its own definition for security breach and conditions for public disclosure. This study does not make explicit claims that the results obtained from RQ2 and RQ3 would be generalizable to other jurisdictions; however, it nonetheless provide a snapshot into current *practice* of disclosure could be a source of scientific knowledge in the current phenomenon of security breach disclosure.

8.1.1 The Definition of Security Breach and The Conditions That Warrant Public Disclosure

From reviewing security breach disclosure requirements, it soon became apparent that there is no current consensus on the definition of security breach and the conditions that would warrant public disclosure. Most regulators have a working definition that requires organizations to disclose incidents that lead to the breach of personal/customer data. However, adopting such limited definitions may cause organizations to neglect the potential harm of other security incidents where no personal data are involved. This study renders two suggestions. First, organizations should thoroughly assess the potential impact of security breaches and establish whether they would cause potential harm to the public; if so, the incident should be disclosed publicly. Second, regulators should encourage organization-specific definition of the term ‘incident’ based on the principle of “*potential harm to the public*” so that the scope of the term is clear. This is because when an incident occurs, it inevitably raises security implications that are unique to the organization’s operation and its involvement in public safety and security. Therefore, organizations need to define their own specific conditions to activate and mobilize certain functions and processes within the organization to handle both the incident and the disclosure effort.

8.1.2 Timing for Disclosure

Except for the EU’s GDPR, which requires organizations to file an initial disclosure within 72 hours of discovery, the majority of current disclosure requirements do not have

a set deadline of disclosure. While some may indicate that disclosures shall be made “within a reasonable time;” this is troubling as it leaves too much room for interpretation. It is generally recognized that law enforcement may require organizations to delay disclosure during active investigation. However, regulators should balance the need of public right-to-know against the need to preserve the integrity of the investigation and provide *both* the organization and the investigative unit proper guidance on the allowed timeframe for delay.

8.1.3 The Lack of Enforcement and Penalties

The lack of enforcement is compounded due to 1) unclear definitions and conditions for public disclosure, 2) Lack of specification on timing of disclosure, and 3) lack of methods to benchmark disclosure for non-compliance. These three issues lead to ambiguities in enforcement, which result in crippled regulations that “have no teeth.” Implementing penalties could encourage organizations to increase their compliance effort, but if the terms of the penalties are also not clearly stated, the regulatory requirement would be perceived by the organizations as “having no bite.” Recent newly proposed laws have started to address the issue of the timing of disclosure; however, it remains to be seen how penalties would be enforced if the benchmark for non-compliance is unclear.

8.1.4 Lack of Disclosures from Non-medical and Non-financial Organizations

As indicated in the descriptive analysis (section 5.5) on the California security breach data, disclosure reports from the financial (22%) and medical (19%) industry accounted

for 41% of all reports filed. Based on the U.S. Small Business Administration Industry Statistics (2015) as presented in Figure 8-1, the number of financial and insurance firms only account for 4%, and the number of healthcare industry organizations account for 11%, for a combined 15%. If we assume the chance that organization, regardless of industry, would encounter security breach at a similar probability, this assumption would predict that reports from healthcare and financial industry would be approximately 15% combined, instead of 41% reported in Table 5-3. While one should not assume that frequency of breach occurrence should be same from industry to industry, one should also consider the possibilities that due to the amount of personal data held by these two industries may also attract more attack. It is also possible that the comparatively low percentage of reports from industries other than financial and healthcare may imply that the existing GLBA and HIPAA regulations certainly make breached organizations “take things more seriously.” However, would the newly proposed U.S. Personal Data Notification and Protection Act have the same effect as GLBA and HIPAA that would make organizations to pay more attention to breach disclosure? This remains to be seen.

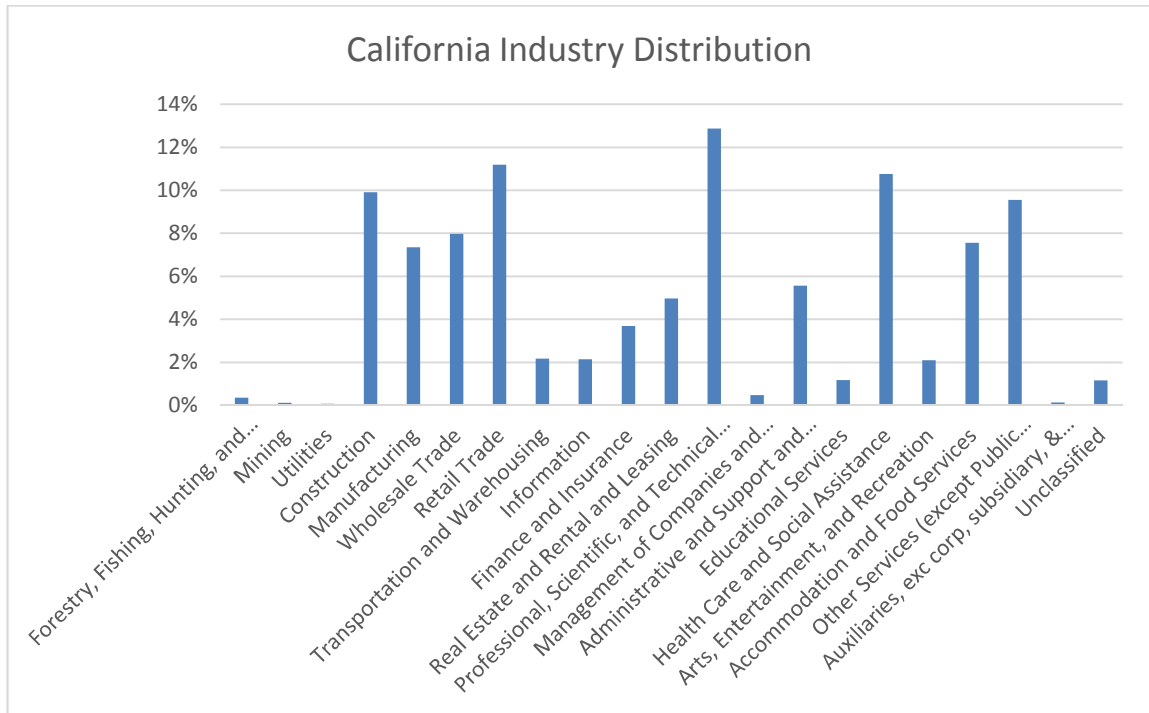


Figure 8-1: California Industry Distribution by Number of Organizations (source: U.S. Small Business Administration Industry Statistics, 2015)

8.1.5 The Information Content of Disclosure

Using the common elements of security breach disclosures found in RQ1, the RQ2 study extracted the information content from security breach disclosures in terms of the descriptions of threat agents, nature of the threats, vulnerability, detection, investigation, impact, and remediation. The results in Figure 5-4 show that the majority of organizations use very little effort to describe vulnerability, which describes what weaknesses were exploited that led to the breach. On average, only 1 out of 4 breaches (0.26) include a description of vulnerability. This implies that organizations are more eager to allocate blame instead of reviewing what weaknesses led to the breach. In

addition, while some organizations diligently describe the breach and provide detailed descriptions of each of the common elements, there exists a wide disparity in organizational efforts as depicted in Figure 5-4. Further investigating this phenomenon, investigations showed that the communications (50%), financial (67%), and insurance (57%) industries had the highest percentage of ambiguous disclosure, which means that no sentence in the report was specifically used to describe a particular element. The results show that the majority of the disclosures in these industries failed to identify who or what was responsible for the security breach. We also found that the reports submitted by the financial industry have, on average, the highest word counts and sentence counts. However, they also have the highest rate of ambiguous reporting. This implies that longer reports do not necessarily translate to higher quality reports.

8.1.6 Different Attitudes toward Internal and External Breaches

From threat agent descriptions, this study further separates internal and external threat agents. The results show that organizations spend more effort on detection and investigation of external threats than they do on internal-sourced threats. In addition, third party involvement, such as law enforcement or external specialists, were found to have a positive correlation with external threats, but a negative correlation was found for internal-sourced threat. These results suggest that organizations are more careful in describing errors and breaches that are caused internally, and less likely to describe the detection, investigation, and third parties involved in external threats. This may be due to organizational affinity to avoid embarrassment by breaches caused by internal agents

indicating that organizational members are involved in potential criminal activity. However, it could also indicate that breaches caused by internal agents are, on average, less severe, requiring less effort concerning the related breach disclosures.

8.1.7 The Quality of Breach Disclosures

In the RQ3 study, three measures of quality were proposed: completeness, time references, and management involvement. In measuring completeness and factors that affect it, this study suggests the following:

- Organizations should spend more effort in describing vulnerability
- C-level management involvement should be encouraged
- Longer reports do not translate into completeness. Organizations should focus on relevant information instead of making disclosure reports longer.
- Allowing organizations more time to prepare disclosures may not result in higher ratings in completeness. This implies that disclosure delays are motivated by factors other than the effort required to prepare the reports.

In terms of timing of disclosure and the existence of time references in the report, this study found that disclosure delays tended to be longer after 2012, the first year that the California regulator began requiring breach disclosure. Further, although this study provided several timeliness measures (see Figure 6-1), the realities of current practice are alarming. There is a general shortage of references to event timing in the report; therefore it is usually unclear on when threats were discovered, when investigations were

started and concluded, and when risk assessment procedures were checked. Lacking inclusion of a detailed timeliness accounting makes it difficult for affected parties to make time-sensitive decisions.

8.2 Research Significance & Contribution

8.2.1 Contribution towards Theory: Exploring and Explaining Issues of Security Breach Disclosure

The expected societal significance of security breach disclosures are profound. Disclosures are an integral process in knowledge transfer and dissemination about organizational capabilities to manage data security problems in the information age. This study explores current theories, policies, and practices and uses actual security breach data to construct a security breach disclosure model that helps to explain the factors, conditions, and incentives surrounding current disclosure practices. To the author's best knowledge, no study of this kind has ever been published on security breach disclosures.

8.2.2 Contribution toward Methodology: Improvements in Extracting Relevant Contents from Security Breach Disclosures

This research provides a better understanding of security incident disclosure requirements and practices and helps to overcome methodological issues in related studies of data breaches. This study included a comprehensive search on security breach disclosures required by various jurisdictions (Stevens, 2012). A two phase approach was used to combine human interpretation and computerized textual-analysis of a large sample of security breach disclosures. In phase one, a grounded theory approach was used to

identify dimensions, constructs, concepts, and context to generate substantive models (Kools et al., 1996) that could be used in phase two. Subsequently, these substantive models were used to guide computerized text-analysis to extract context-specific (Adomavicius et al., 2011) and semantic-meaningful (Cambria et al., 2013; 2014) data from a large sample of unstructured security breach disclosure data. From the evidence gathered, this study employed statistical techniques to analyze the patterns and theorize a model that enhances our understanding of the role of breach disclosure in the prevention, detection, investigation, and remediation of processes in ISM.

8.2.3 Provision of a Theoretical Foundation for Future Cyber Security Studies

To establish the theoretical model and framework, this study reviewed theories in economics, behavioral science, and information systems. Building on existing work in these disciplines, these theories were applied in the context of security breach disclosure. This theoretical foundation will support future studies on the issues of security breach disclosure, thus contributing towards knowledge building in the field of information security management.

8.2.4 Informing Practice and Policy on the Quality Domains of Security Breach Disclosure and Causal Conditions That Affect the Quality of Disclosure:

This research provides valuable insight that can be used by businesses and policymakers as they develop policies and best practices for information security and data breach

response. The overall objective of security breach disclosure requirements from the government's perspective is to ensure that individuals are informed when their personal information has been compromised and that they have been put at risk of harm, so that they can take steps to protect themselves and mitigate the harm. Proper disclosure allows the security industry to obtain relevant information on security incidents so that new tools can be developed for discovery, detection, investigation, and mitigation of security breaches.

Cyberattacks continue to increase in frequency and sophistication, presenting significant challenges for organizations that must defend their data and systems from capable threat agents. These threat agents range from individual, autonomous attackers to well-resourced groups operating as criminal enterprises or on behalf of nation-states. Threat actors can be persistent, motivated, and agile, and they use a variety of tactics, techniques, and procedures to cause security incidents. These incidents can result in compromised systems and disrupted services, allowing threat agents to commit financial fraud and expose or steal intellectual property and other sensitive information.

Given the risks these threats present and the continual evolution of tools and techniques used by threat agents, it is increasingly important that organizations properly disclose information regarding breaches. Effective security breach disclosure can help organizations improve their security posture, and help stakeholders to identify, assess, monitor, and respond to cyber threats. Examples of security breach disclosure can include not only basic information for affected individuals. It can also include security alerts,

threat intelligence reports, and recommended remediation actions. Most organizations already produce multiple types of cyber threat information that are available for internal disclosure as part of their incident response management process and security operations efforts. By properly disclosing breach information throughout the community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face.

Using the knowledge accumulated and transferred, an organization can make informed decisions regarding defensive capabilities, threat detection techniques, investigation plans, and mitigation strategies. By correlating and analyzing information on threat agents and vulnerabilities from multiple sources, organizations can also enrich existing information and make it more actionable. In addition, sharing of threat information through disclosure allows organizations to better detect threats that target particular industry sectors, business entities, or institutions.

This study can assist policy makers, practitioners, and future researchers to develop an understanding of the issues surrounding security breach disclosure. The study's contribution includes a description of the current policies, practices, and challenges of breach disclosure. It also clarifies the current landscape of security breach disclosure, and introduces an analytical framework that considers the roles, factors, and conditions that affect disclosure. The goal of the study has been to provide the theoretical underpinning

needed to improve security breach disclosure policies, practices, and to enable future research in this field.

8.3 Recommendations towards Better Breach Disclosure Practices

Generally, the goals of security breach disclosure include:

- 1) Ensure that threat agents and vulnerabilities can be identified and controlled effectively and efficiently for all parties.
- 2) Minimize the potential impact to the parties affected; reduce the risks that could allow further damage to their systems.
- 3) Provide affected parties with sufficient information for them to evaluate the impact of the breach.
- 4) Knowledge accumulation: Provide the organization and the public with the information necessary to develop tools and methods for identifying, managing, and reducing the risks of future breach.

To accomplish these goals, it is crucial to consider how breach reporting requirements are specified, enforced, and how information contained in breach disclosure are communicated to the relevant stakeholders and shared among the information security community. Based on findings in this study, the following recommendations are provided for considerations:

Proactively establish security breach disclosure policies and definitions. It could be difficult for regulator to establish a general definition for security breach and set a conditions for public disclosure that would encompass all different type of organizations. Rather than simply attempting to follow definitions set by regulators, management should also build on these definitions and regulations to establish organization-specific definitions for security incidents, security breaches, and conditions for public disclosure. This would encourage management to be cognizant of the organization's responsibility in protecting customer data and be proactive in consider the potential to cause harm if certain data are lost.

Organizations should plan ahead and have internal procedures in place before incidents occur. Such advanced planning helps ensure that participating organizations and internal employees understand their roles, responsibilities, and information handling requirements before, during, and after a security breach.

Encourage senior management involvement and support. Results in this study shows statistically significant evidence that senior management involvement are positively associated with breach report completeness, third party involvement, and overall quality of breach report. While the results also shows a positive association with report delay; however, it signals that breach reports are treated more carefully. While none of the current regulations require senior management sign-off on breach disclosure, it is nonetheless important in terms of improving the quality of security breach disclosure.

Establish internal security breach disclosure policy and guideline. External disclosure regulations are intended to control the publication and distribution of threat information, and consequently help to prevent the dissemination of information that, if improperly disclosed, may have adverse consequences for an organization, its customers, or its business partners. However, if the external disclosure regulations are not considered and implemented through internal disclosure policies and guidelines, the responsibilities of reporting and extent of detail could be subject to management discretion, thereby negatively impact the quality of breach disclosure.

Actively seek to enrich disclosure by providing relevant content. When possible, organizations should increase the usefulness and effectiveness of breach disclosure by producing relevant information in terms of threat agent, nature of threat, vulnerability, detection, investigation, impact, and remediation. These core elements, as suggested by this study, can provide essential information describing the incident such that each core elements can be studied by the organization and by the information security community as a whole for the development of new tools and strategies. In addition, this study finds evidence that longer reports do not contribute towards disclosure quality, and the use of “fluff”, such as sentences that associate with “apology”, has no statistical significant effect on the quality of breach disclosure.

Establish workflows to publish, consume, analyze, and act upon new threat information. This study suggests use of standardized data formats (XML) to disclosure security breach. The use of standardized, structured, and pre-formatted data format to

publish breach information could make it easier to automate breach information processing. The positive benefits include allowing regulators to quickly evaluate compliance effort, enabling organizations to quickly compare its disclosure practices against other organizations, and enhance the information security community's ability to consume the data. The use of automation enabled by structured reporting enables cyber threat information to be rapidly shared, transformed, enriched, analyzed, and acted upon with less need for manual intervention.

8.4 Threat Information Sharing through Disclosure

For practitioners, breach disclosure provides access to threat information, investigation and remediation efforts that might otherwise be unavailable to an organization. The accumulation of knowledge thus contributes towards a shared resources of relevant information regarding security events that organizations can use to enhance their security posture by leveraging the knowledge, experience, and capabilities shared through committed disclosure practices in a proactive way through the information security community.

Shared Situational Awareness. The sharing and learning of security breach disclosure enables organizations to leverage the collective knowledge, experience, and analytic capabilities within the information security community. The proactive sharing and learning of security breach disclosure can increase the situational awareness and security of an entire community.

Improved Security Posture. By developing and sharing threat information, organizations gain a better understanding of the threat environment and can use threat information to inform their security and risk management practices. Using shared information, organizations can identify affected platforms or systems, implement protective measures, enhance detection capabilities, and more effectively respond and recover from incidents based on observed changes in the threat environment. As organizations share breach information and subsequently learn from the accumulated knowledge through the information security community, those organizations can improve their overall security posture.

Knowledge Maturation. When seemingly unrelated security incidents and observations are shared and analyzed by organizations and by the information security community, those observations can be correlated with data collected by others. This enrichment process enhanced by robust security breach disclosure practices increases our understanding and ability to develop new tools, strategies, and countermeasures for new incidents, threats, or threat agents. The knowledge maturation through the learning and cooperation between the information security community and management are the final goals of this study.

REFERENCES

- Ablon, L., Heaton, P., Lavery, D. C., & Romanosky, S. (2016). Consumer attitudes toward data breach notifications and loss of personal information. Rand Corporation.
- Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation.
- Aboody, D., & Kasznik, R. (2000). CEO stock option awards and the timing of corporate voluntary disclosures. *Journal of accounting and economics*, 29(1), 73-100.
- Acquisti, A., Friedman, A. and Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study. Fifth Workshop on the Economics of Information Security. Jun. 26.
- Aggarwal, C. C., & Zhai, C. (2012). Mining text data. Springer Science & Business Media.
- Akerlof, G. A. (1978). The market for “lemons”: Quality uncertainty and the market mechanism. In *Uncertainty in Economics* (pp. 235-251).
- Ali, J., & Santos, J. R. (2015). Modeling the Ripple Effects of IT - Based Incidents on Interdependent Economic Systems. *Systems Engineering*, 18(2), 146-161.
- Allodi, L. (2017). Economic Factors of Vulnerability Trade and Exploitation. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1483-1499). ACM.
- ALM Intelligence (2017). Risk + Crisis Management in-depth Report. Morrison Foerster.
- Amernic, J., Craig, R., & Tourish, D. (2010). Measuring and assessing tone at the top using annual report CEO letters. The Institute of Chartered Accountants of Scotland.

- Anderson, R. (2001). Why information security is hard-an economic perspective. In Computer security applications conference, 2001. ACSAC 2001. Proceedings 17th annual (pp. 358-365). IEEE.
- Anderson, R. (2002). Security in open versus closed systems—the dance of Boltzmann, Coase and Moore. Technical report, Cambridge University, England.
- Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610-613.
- Anderson, R., & Moore, T. (2009). Information security: where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 367(1898), 2717-2727.
- Anderson, R., Böhme, R., Clayton, R., & Moore, T. (2009). Security economics and European policy. In *Managing information risk and the economics of security* (pp. 55-80). Springer, Boston, MA.
- Andoh-Baidoo, F. K., & Osei-Bryson, K. M. (2007). Exploring the characteristics of Internet security breaches that impact the market value of breached organizations. *Expert Systems with Applications*, 32(3), 703-725.
- Andrijcic, E., & Horowitz, B. (2006). A Macro - Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property. *Risk Analysis*, 26(4), 907-923.
- Armerding, T. (2018) The 17 biggest data breaches of the 21st century. Retrieved May 1st, 2018, from <https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html>
- Arora, A., & Telang, R. (2005). Economics of software vulnerability disclosure. *IEEE security & privacy*, 3(1), 20-25.

- Arora, A., Telang, R., & Xu, H. (2008). Optimal policy for software vulnerability disclosure. *Management Science*, 54(4), 642-656.
- Arora, A., Krishnan, R., Telang, R., & Yang, Y. (2010). An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure. *Information Systems Research*, 21(1), 115-132.
- Ansoff, H. I. (1965). *Corporate strategy: business policy for growth and expansion*. McGraw-Hill Book.
- Baker, G., Gibbons, R., & Murphy, K. J. (1994). Subjective performance measures in optimal incentive contracts. *The Quarterly Journal of Economics*, 109(4), 1125-1156.
- BakerHostetler (2017) Data Breach Charts. BakerHostetler. Retrieved May 1st, 2018 from
https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf
- Ballou, D. P., & Pazer, H. L. (1995). Designing information systems to optimize the accuracy-timeliness tradeoff. *Information Systems Research*, 6(1), 51-72.
- Barber, R. (2001). Hacking techniques: The tools that hackers use, and how they are evolving to become more sophisticated. *Computer Fraud & Security*, 2001(3), 9-12.
- Bauer, J. M., & Van Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10), 706-719.
- Bensinger G. and McMillan, R. (2017). Uber Reveals Data Breach and Cover-up, Leading to Two Firings. *The Wall Street Journal*. Retrieved May 1st, 2018 from
<https://www.wsj.com/articles/uber-reveals-data-breach-and-cover-up-leading-to-two-firings-1511305453>

- Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International journal of contemporary hospitality management*, 24(7), 991-1010.
- Bergstresser, D., & Philippon, T. (2006). CEO incentives and earnings management. *Journal of financial economics*, 80(3), 511-529.
- Berry, M. W. (2004). Survey of text mining. *Computing Reviews*, 45(9), 548.
- Birks, D. F., Fernandez, W., Levina, N. and Nasirin, S. (2013). Grounded theory method in information systems research: its nature, diversity and Opportunities, *European Journal of Information Systems* (2013) 22, 1–8.
- Bloomberg (2017). Three Equifax Managers Sold Stock Before Cyber Hack Revealed. September 7, 2017. Retrieved May 1st, 2018 from <https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack>
- Bloomberg (2018). Facebook Finds Ongoing Evidence of Election Interference. July 31, 2018. Retrieved August 13st, 2018 from <https://www.bloomberg.com/news/articles/2018-07-31/facebook-finds-ongoing-evidence-of-election-interference>
- Blumenthal, R. & McSweeney, T. (2017) If you're not angry about Equifax, you should be. CNN. Retrieved May 1st, 2018 from <https://www.cnn.com/2017/09/26/opinions/congress-protect-americans-from-security-breaches-blumenthal-mcsweeney-opinion/index.html>
- Botosan, C. A. (1997). Disclosure level and the cost of equity capital. *Accounting review*, 323-349.

- Botosan, C. A., & Plumlee, M. A. (2002). A re - examination of disclosure level and the expected cost of equity capital. *Journal of accounting research*, 40(1), 21-40.
- Bowen, P., Hash, J., & Wilson, M. (2007). Information security handbook: a guide for managers. In NIST Special Publication 800-100, National Institute of Standards and Technology.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.
- Burstein A. & Mulligan D. (2007) Security Breach Notification Laws: Views from Chief Security Officers. Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law.
- Campbell, K., Gordon, L., Loeb, L., and Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the stock market. *Journal of Computer Security*, 11(3) 431-448
- Cárdenas, A., Radosavac, S., Grossklags, J., Chuang, J., & Hoofnagle, C. (2009). An economic map of cybercrime.
- Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International J. of Electronic Commerce* 9(1).
- Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2005). Emerging Issues in Responsible Vulnerability Disclosure. In WEIS.
- Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, 50(4), 651-661.

- Chen, R. (2018) Combating data breach fatigue. Phys.org Retrieved May 1st, 2018 from <https://phys.org/news/2018-01-combating-breach-fatigue.html>
- Chomsky, N., & Lightfoot, D. W. (2002). Syntactic structures. Walter de Gruyter.
- Chow, C. C., & Sarin, R. K. (2002). Known, unknown, and unknowable uncertainties. *Theory and Decision*, 52(2), 127-138.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. NIST Special Publication, 800(61), 1-147.
- Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling theory: A review and assessment. *Journal of management*, 37(1), 39-67.
- Congressional Research Service (2012). Data Security Breach Notification Laws. United States Congress
- Corbin, J., & Strauss, A. (1990). Grounded theory research: Procedures, canons and evaluative criteria. *Zeitschrift für Soziologie*, 19(6), 418-427.
- CyberArk (2018). CyberArk Global Advanced Threat Landscape Report 2018. CyberArk.
- Debreceeny, R., & Gray, G. L. (2001). The production and use of semantically rich accounting reports on the Internet: XML and XBRL. *International Journal of Accounting Information Systems*, 2(1), 47-74.
- Department of Treasury (2005). Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.
- Ding, C., & He, X. (2004, July). K-means clustering via principal component analysis. In *Proceedings of the twenty-first international conference on Machine learning* (p. 29). ACM.

- Dogan, Mustafa, Coskun, Ender, Orhan, Celik (2007): “Is timing of financial reporting related to firm performance? -An examination on ISE listed companies”, International research journal of finance and economics, issue 12, p.220-233
- Doidge, C., Karolyi, G. A., & Stulz, R. M. (2007). Why do countries matter so much for corporate governance?. Journal of financial economics, 86(1), 1-39.
- Dranove, D., & Jin, G. Z. (2010). Quality disclosure and certification: Theory and practice. Journal of Economic Literature, 48(4), 935-63.
- Dye, R. A. (1985). Disclosure of nonproprietary information. Journal of accounting research, 123-145.
- Earle, B. H., & Madek, G. A. (2007). The Mirage of Whistleblower Protection Under Sarbanes - Oxley: A Proposal for Change. American Business Law Journal, 44(1), 1-54.
- Edelman, B. (2009). Adverse selection in online trust certifications. In Proceedings of the 11th International Conference on Electronic Commerce (pp. 205-212). ACM.
- Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. Journal of Cybersecurity, 2(1), 3-14.
- Fairclough, N. (2003). Analysing discourse: Textual analysis for social research. Psychology Press.
- Federal Bureau of Investigation (2017). Internet Crime Report. U.S. Department of Justice.
- Furnell, S., & Thomson, K. L. (2009). Recognising and addressing ‘security fatigue’. Computer Fraud & Security, 2009(11), 7-11.

- Gasson, S. (2004). Rigor in grounded theory research: An interpretive perspective on generating theory from qualitative field studies. In *The handbook of information systems research* (pp. 79-102). IGI Global.
- Glaser, B. G. (1978). Theoretical sensitivity: Advances in the methodology of grounded theory. *Sociology Pr.*
- Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, 46(7), 404-410.
- Goel, S., & Shawky, H. A. (2014). The Impact of Federal and State Notification Laws on Security Breach Announcements. *CAIS*, 34, 3.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, 25(5), 503-530.
- Grance, T., Kent, K., & Kim, B. (2004). Computer security incident handling guide. NIST Special Publication, 800(61), 11.
- Grachis, G. (2017) A look back at cybersecurity in 2017.CSO online. Retrieved May 1st, 2018 from <https://www.csoonline.com/article/3239405/data-breach/a-look-back-at-cybersecurity-in-2017.html>
- Graham, John R. (2005):”The economic implications of corporate financial reporting”, *Journal of accounting and economics*, vol.40, p.3-73
- Harrell, E., & Langton, L. (2013). Victims of identity theft, 2012 (p. 12). US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.
- Harrell, E. (2015). Victims of identity theft, 2014. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

- Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of accounting and economics*, 31(1-3), 405-440.
- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.
- Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-Risk Disclosure: Who Cares?.
- Hovav, A., & D'Arcy, J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security*, 13(3), 32-40.
- ITRC (2016). 2016 end of year data breach reports. Identity Theft Resource Center.
- Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Congressional Research Service, Library of Congress.
- Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, 12(1), 69-91.
- Knapp, E. D., & Langill, J. T. (2014). Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Syngress.
- Ferraro, M. F. (2013). Groundbreaking or Broken; An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications. *Alb. L. Rev.*, 77, 297.
- Freeman, R. E. (2010). Strategic management: A stakeholder approach. Cambridge university press.

- Furnell, S., & Thomson, K. L. (2009). Recognising and addressing 'security fatigue'. *Computer Fraud & Security*, 2009(11), 7-11.
- Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT Security Breaches: what do investors think?. *Information Systems Security*, 12(1), 22-33.
- Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, 11(2), 74-83.
- Garrison, L., M. Hastak, J. M. Hogarth, S. Kleimann, and A. S. Levy, "Designing Evidence - Based Disclosures: A Case Study of Financial Privacy Notices," *Journal of Consumer Affairs*, Vol. 46, No. 2, 2012, pp. 204–234.
- Gaziano, C., & McGrath, K. (1986). Measuring the concept of credibility. *Journalism quarterly*, 63(3), 451-462.
- Ge, W., & McVay, S. (2005). The disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act. *Accounting Horizons*, 19(3), 137-158.
- Gigler, F. B., & Hemmer, T. (2001). Conservatism, optimal disclosure policy, and the timeliness of financial reports. *The Accounting Review*, 76(4), 471-493.
- Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, 46(7), 404-410.
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security*, 19(1), 33-56.
- Government Accountability Office, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; however the Full Extent is Unknown; Washington, D.C., GAO-07-737, 2007.

- Grant, G. H., & Grant, C. T. (2014). SEC cybersecurity disclosure guidance is quickly becoming a requirement. *The CPA Journal*, 84(5), 69.
- Grady, M. F., & Parisi, F. (Eds.). (2005). *The law and economics of cybersecurity*. Cambridge University Press.
- Halzack, Sarah, (2014). Home Depot and JPMorgan Are Doing Fine. Is It a Sign We're Numb to Data Breaches? *Washington Post*, October 6, 2014. Retrieved May 1st, 2018 from <http://www.washingtonpost.com/news/get-there/wp/2014/10/06/home-depot-and-jpmorgan-are-doing-fine-is-it-a-sign-were-numb-to-data-breaches/>
- Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of accounting and economics*, 31(1-3), 405-440.
- Hearit, K. M. (2006). *Crisis management by apology: Corporate response to allegations of wrongdoing*. Routledge.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.
- Herr, T., & Romanosky, S. (2015). *Cyber crime: security under scarce resources*.
- Humpherys, S. L., Moffitt, K. C., Burns, M. B., Burgoon, J. K., & Felix, W. F. (2011). Identification of fraudulent financial statements using linguistic credibility analysis. *Decision Support Systems*, 50(3), 585-594.
- Javelin Strategy and Research, 2011 Identity Fraud Survey Report: Consumer Version, Pleasanton, Calif., February 2011.

- Jung, W. O., & Kwon, Y. K. (1988). Disclosure when the market is unsure of information endowment of managers. *Journal of Accounting research*, 146-153.
- Kan, M. (2017) Yahoo execs botched its response to 2014 breach, investigation finds. CSO online. Retrieved May 1st, 2018 from <https://www.csoonline.com/article/3176181/security/yahoo-execs-botched-its-response-to-2014-breach-investigation-finds.html>
- Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, 12(1), 69-91.
- Kincaid, J. P., Fishburne Jr, R. P., Rogers, R. L., & Chissom, B. S. (1975). Derivation of new readability formulas (automated readability index, fog count and flesch reading ease formula) for navy enlisted personnel.
- Ko, M. , & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, 17, 13–22.
- Kools, S., McCarthy, M., Durham, R., & Robrecht, L. (1996). Dimensional analysis: Broadening the conception of grounded theory. *Qualitative Health Research*, 6(3), 312-330.
- Kothari, S. P., Shu, S., & Wysocki, P. D. (2009). Do managers withhold bad news?. *Journal of Accounting Research*, 47(1), 241-276.
- Kuehn, A., & Mueller, M. (2014). Shifts in the Cybersecurity Paradigm: Zero-Day Exploits, Discourse, and Emerging Institutions. In *Proceedings of the 2014 New Security Paradigms Workshop* (pp. 63-68). ACM.

- Kulynych, J., & Korn, D. (2003). The new HIPAA (Health Insurance Portability and Accountability Act of 1996) Medical Privacy Rule: help or hindrance for clinical research?. *Circulation*, 108(8), 912-914.
- Laube, S., & Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, 2(1), 29-41.
- Lee, Ho-Young, Mande, Vivek and Son, Myungsoo (2008): “A comparison of reporting lags of multinational and domestic firms”, *Journal of international financial management and accounting*, 19:1, p.28-56
- Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS quarterly*, 71-90.
- Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.
- Los Angeles Times. (2017). Before its massive data breach, Equifax fought to kill a rule allowing victims to sue. September 11, 2017. Retrieved May 1st, 2018 from <http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-arbitration-20170911-story.html>
- Lanz, J. (2014). Cybersecurity governance: The role of the audit committee and the CPA. *The CPA Journal*, 84(11), 6.
- Levin, Adam, “How This Federal Data Breach Law Could Actually Hurt Consumers,” *Forbes*, March 27, 2015. <http://www.forbes.com/sites/adamlevin/2015/03/27/how-this-federal-data-breach-law-could-actually-hurt-consumers>
- Lewis, T. G. (2014). *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons.

- Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS quarterly*, 71-90.
- Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394.
- Lev, B. (1992). Information disclosure strategy. *California Management Review*, 34(4), 9-32.
- Libicki, Martin C., Lillian Ablon, and Tim Webb, *The Defender's Dilemma: Charting a Course Toward Cybersecurity*, Santa Monica, Calif.: RAND Corporation, RR-1024-JNI, 2015. Retrieved May 1st, 2018 from http://www.rand.org/pubs/research_reports/RR1024.html
- Lord, B (2016) An Important Message about Yahoo User Security. Yahoo! Inc. Retrieved May 1st, 2018 from <https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security>
- Madden, M. (2014). Public perceptions of privacy and security in the post-Snowden era. Pew Research Center, 12.
- Madden, M., & Rainie, L. (2015). Americans' attitudes about privacy, security and surveillance. Pew Research Center.
- Mahajan, Poonam and Chander, Subhash (2008): "Determinants of timeliness of corporate disclosure of selected companies in india", *ICFAI journal of accounting research*, vol.7, issue 4, p.28-63
- Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security*, 2013(6), 9-13.

- McCrack, J. & Finkle, J. (2018). Equifax breach could be most costly in corporate history. Reuters. Retrieved May 1st, 2018 from <https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257>
- Meyer, P. (1988). Defining and measuring credibility of newspapers: Developing an index. *Journalism quarterly*, 65(3), 567-574.
- Meyers, C. A., Powers, S. S., & Faissol, D. M. (2009). Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches (No. LLNL-TR-419041). Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States).
- Mitra, S., & Ransbotham, S. (2012). The effects of vulnerability disclosure policy on the diffusion of security attacks. In *Thirty Third International Conference on Information Systems*, Orlando 2012 (pp. 1-17).
- Moore, T., & Anderson, R. (2011). *Economics and Internet Security: A Survey of Recent Analytical, Empirical, and Behavioral Research*.
- Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, 3(3-4), 103-117.
- Milligan, D., Hoofnagle, C. (2007) Identity Theft: Innovative Solutions for an Evolving Problem: Hearing Before the Subcomm. on Terrorism, Technology and Homeland Security of the Senate Committee On the Judiciary, 110th U.S. Congress. <http://judiciary.senate.gov/pdf/3-21-07HoofnagleTestimony.pdf>.
- Odlyzko, A. (2003). Privacy, economics, and price discrimination on the internet. In *Proceedings of the 5th international conference on electronic commerce* (pp. 355–366). New York: ACM
- Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. Pew Research Center, 1-5.

- O'Reilly III, C. A. (1982). Variations in decision makers' use of information sources: The impact of quality and accessibility of information. *Academy of Management journal*, 25(4), 756-771.
- Orlov, D. (2015). Optimal design of internal disclosure. SSRN
- OWASP (2012). OWASP Application Security Guide For CISO Project. The Open Web Application Security Project. Retrieved May 1st,2018 from https://www.owasp.org/index.php/CISO_AppSec_Guide:Criteria_for_Managing_Application_Security_Risks
- Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on* (pp. 156b-156b). IEEE.
- Perlberg, S., “Do Consumers Have Data Breach Fatigue?” *Wall Street Journal*, October 9, 2014. Retrieved May 1st,2018 from <http://blogs.wsj.com/cmo/2014/10/09/data-breach-impact-yougov>
- Pinsker, R., & Li, S. (2008). Costs and benefits of XBRL adoption: Early evidence. *Communications of the ACM*, 51(3), 47-50.
- Polinsky, A. M., & Shavell, S. (2010). Mandatory versus voluntary disclosure of product risks. *The Journal of Law, Economics, & Organization*, 28(2), 360-379.
- Ponemon (2017) Ponemon 2017 Cost of Data Breach Study. IBM. Retrieved May 1st,2018 from <https://www.ibm.com/security/data-breach>
- Porter, C., Krogulski, J., & Drum, S. (2018). Responding to GDPR pushback: The business case for compliance. International Association of Privacy Professionals. Retrieved May 1st,2018 from <https://iapp.org/news/a/responding-to-gdpr-pushback-the-business-case-for-compliance/>

- Regan, P. M. (2009). Federal Security Breach Notifications: Politics and Approaches. *Berkeley Tech. LJ*, 24, 1103.
- Rescorla, E. (2003). Security holes... Who cares?. In *USENIX Security Symposium* (pp. 75-90).
- Rescorla, E. (2005). Is finding security holes a good idea?. *IEEE Security & Privacy*, 3(1), 14-19.
- Reuters (2017) Yahoo says all three billion accounts hacked in 2013 data theft. Reuters, Oct. 3, 2017. <https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1>
- Romanosky, S., & Acquisti, A. (2009). Privacy costs and personal data protection: Economic and legal perspectives. *Berkeley Technology Law Journal*, 24(3), 1061-1101.
- Romanosky, S., Acquisti, A., & Sharp, R. (2010). Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal? SSRN.
- Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, 11(1), 74-104.
- Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft?. *Journal of Policy Analysis and Management*, 30(2), 256-286.
- Ransbotham, S. & Mitra, S. (2009) Choice and Chance: A Conceptual Model of Paths to Information Security Compromise, *Information Systems Research*, Vol. 20, No. 1, March 2009, pp. 121–139
- Schneier, B. (2000). Full disclosure and the window of vulnerability. *Crypto-Gram* Retrieved May 1st, 2018 from <http://www.counterpane.com/crypto-gram-0009.html>

- Schwartz, P. M., & Janger, E. J. (2007). Notification of data security breaches. *Michigan Law Review*, 913-984.
- Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, 32(2), 314-341.
- Shepherd, S. (2003). Vulnerability Disclosure: How Do We Define Responsible Disclosure?. GIAC SEC Practical Repository, SANS Institute.
- Shey H., Balaouras, S., Holland R. Duong, J., Spillotes, A., & Dostie, P. (2015) Market Overview: Customer Data Breach Notification And Response Services. Forrester.
- Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.
- Skinner, D. J. (1994). Why firms voluntarily disclose bad news. *Journal of accounting research*, 32(1), 38-60.
- Stagliano, A. J., & Sillup, G. P. (2014). Transparency and risk assessment reporting: A case study sector survey of cybercrime disclosures. *Journal of Business and Economics*, 5(7), 1134-1140.
- Stefan Laube and Rainer Böhme (2016), The Economics of Mandatory Security Breach Reporting to Authorities, *Journal of Cyber Security*, 2(1) 29-41.
- Sullivan, R. J., & Maniff, J. L. (2016). Data breach notification laws. *Economic Review-Federal Reserve Bank of Kansas City*, 101(1), 65.
- Tang, M., Alazab, M., & Luo, Y. (2017). Big Data for Cybersecurity: Vulnerability Disclosure Trends and Dependencies. *IEEE Transactions on Big Data*.

- Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *Software Engineering, IEEE Transactions on*, 33(8), 544-557.
- The Guardian. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. March 17, 2018. Retrieved May 1st, 2018 from <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- The Wall Street Journal (2016). Should Companies Be Required to Share Information About Cyberattacks? The Wall Street Journal May 22, 2016. Retrieved May 1st, 2018 from <https://www.wsj.com/articles/should-companies-be-required-to-share-information-about-cyberattacks-1463968801>
- The Wall Street Journal (September, 2017). Equifax Lobbied for Easier Regulation Before Data Breach. The Wall Street Journal, September 11, 2017. Retrieved May 1st, 2018 from <https://www.wsj.com/articles/equifax-lobbied-for-easier-regulation-before-data-breach-1505169330>
- The Wall Street Journal (October, 2017). Former Equifax CEO Faces Congress. The Wall Street Journal, October 4, 2017. Retrieved May 1st, 2018 from <https://www.wsj.com/livecoverage/equifax-hack-hearing-1003>
- Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers & security*, 24(2), 105-108.
- Tsukayama, H. (2017). Equifax faces hundreds of class-action lawsuits and an SEC subpoena over the way it handled its data breach. *Washington Post*. Retrieved May 1st, 2018 from https://www.washingtonpost.com/news/the-switch/wp/2017/11/09/equifax-faces-hundreds-of-class-action-lawsuits-and-an-sec-subpoena-over-the-way-it-handled-its-data-breach/?utm_term=.22b1a3299c10

- U.S. Office of the Press Secretary, (2015). Fact Sheet: Safeguarding American Consumers and Families, White House. Retrieved May 1st, 2018 from <https://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families>
- U.S. Congress, 1st Session, Data Security and Breach Notification Act of 2015, Senate Bill 177, January 13, 2015a. Retrieved May 1st, 2018 from <https://www.congress.gov/bill/114th-congress/senate-bill/177/text>
- Ussahawanitchakit, Phapruke (2011): "Disclosure quality, corporate citizenship and corporate image: evidence from Thai listed companies", International journal of business research, vol.11, no.4, p.1-8
- Veltsos, J. R. (2012). An analysis of data breach notifications as negative news. Business Communication Quarterly, 75(2), 192-207.
- Verizon (2014). Data Breach Investigations Report, 2014. Verizon
- Verizon (2017). Data Breach Investigations Report, 2017. Verizon
- Verrecchia, R. E. (1983). Discretionary disclosure. Journal of accounting and economics, 5, 179-194.
- Verrecchia, R. E. (1990). Information quality and discretionary disclosure. Journal of accounting and Economics, 12(4), 365-380.
- Verrecchia, R. E. (2001). Essays on disclosure. Journal of accounting and economics, 32(1-3), 97-180.
- Vishik, C., Sheldon, F., & Ott, D. (2013). Economic incentives for cybersecurity: Using economics to design technologies ready for deployment. In ISSE 2013 Securing Electronic Business Processes (pp. 133-147). Springer Vieweg, Wiesbaden

- Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), 371-376.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102.
- Wang, J., Xiao, N., & Rao, H. R. (2010). Drivers of information security search behavior: An investigation of network attacks and vulnerability disclosures. *ACM Transactions on Management Information Systems (TMIS)*, 1(1), 3.
- Wash, R., & Rader, E. J. (2015, July). Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *SOUPS* (pp. 309-325).
- West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., & Ruefle, R. (2003). Handbook for computer security incident response teams (csirts) (No. CMU/SEI-2003-HB-002). Carnegie-mellon University.
- Michalski, R. S., Carbonell, J. G., & Mitchell, T. M. (Eds.). (2013). *Machine learning: An artificial intelligence approach*. Springer Science & Business Media.
- Wikina, S. B. (2014). What caused the breach? an examination of use of information technology and health data breaches. *Perspectives in health information management*, 11(Fall).
- Wong, J. C. (2017). Uber concealed massive hack that exposed data of 57m users and drivers. Retrieved May 1st, 2018 from <https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack>
- Wong, R. (2013). European Data Protection Supervisor's Opinion on Cybersecurity. In *Data Security Breaches and Privacy in Europe* (pp. 35-37). Springer, London.

- Wright, R. (2017). Proposed data breach legislation could put executives in jail. Retrieved May 1st, 2018 from <https://searchsecurity.techtarget.com/news/450431197/Proposed-data-breach-legislation-could-put-executives-in-jail>
- Yahoo! Inc. (2014). Form 10-K 2013. SEC EDGAR. Retrieved May 1st, 2018 from <http://www.sec.gov/edgar.shtml>
- Yahoo! Inc. (2016) Yahoo 2013 Account Security Update FAQs. Retrieved May 1st, 2018 from <https://help.yahoo.com/kb/account/SLN28451.html?impressions=true>
- Yahoo! Inc. (2017). Form 10-K 2016. SEC EDGAR. Retrieved May 1st, 2018 from <http://www.sec.gov/edgar.shtml>
- Yayla, A., & Hu, Q. (2005). The impact of security breaches on the value of stocks: a short-term vs. long-term perspective. In Proceedings of the Annual Conference of IS in Asia-Pacific (ISAP 2005), December (Vol. 10).
- Yoon, H., Zo, H., & Ciganek, A. P. (2011). Does XBRL adoption reduce information asymmetry?. Journal of Business Research, 64(2), 157-163.

APPENDIX

APPENDIX 1 – EU SECURITY BREACH NOTIFICATION CONTENT REQUIREMENTS. (TO GOVERNING AUTHORITY)

Section 1- Identification of the provider

1. Name of the provider
2. Identity and contact details of the data protection officer or other contact point where more information can be obtained
3. Whether it concerns a first or second notification

Initial information on the personal data breach (for completion in later notifications, where applicable)

4. Date and time of incident (if known; where necessary an estimate can be made), and of detection of incident
5. Circumstances of the personal data breach (e.g. loss, theft, copying)
6. Nature and content of the personal data concerned
7. Technical and organizational measures applied (or to be applied) by the provider to the affected personal data
8. Relevant use of other providers (where applicable)

Section 2 - Further information on the personal data breach

9. Summary of the incident that caused the personal data breach (including the physical location of the breach and the storage media involved):

10. Number of subscribers or individuals concerned

11. Potential consequences and potential adverse effects on subscribers or individuals

12. Technical and organizational measures taken by the provider to mitigate potential adverse effects

Possible additional notification to subscribers or individuals

13. Content of notification

14. Means of communication used

15. Number of subscribers or individuals notified

Possible cross-border issues

16. Personal data breach involving subscribers or individuals in other Member States

17. Notification of other competent national authorities

**APPENDIX 2 – EU SECURITY BREACH NOTIFICATION
CONTENT REQUIREMENTS (Content of the notification to the
subscriber or individual)**

1. Name of the provider
2. Identity and contact details of the data protection officer or other contact point where more information can be obtained
3. Summary of the incident that caused the personal data breach
4. Estimated date of the incident
5. Nature and content of the personal data concerned as referred to in Article 3(2)
6. Likely consequences of the personal data breach for the subscriber or individual concerned as referred to in Article 3(2)
7. Circumstances of the personal data breach as referred to in Article 3(2)
8. Measures taken by the provider to address the personal data breach
9. Measures recommended by the provider to mitigate possible adverse effects

APPENDIX 3 – United Kingdom Information Commissioner’s Office (ICO) Notification of Privacy and Electronic Communications Regulations (PECR) security breaches

Initial notification (within 24 hours) - must always include the following summary information:

- The name of the service provider.
- The name and contact details of the data protection officer or other contact point where more information can be obtained.
- Whether it is an initial notification or a full notification.
- The date and time of the breach (or an estimate) and the date and time of detection.
- The circumstances of the breach (e.g. theft, loss, copying).
- The nature and content of the personal data concerned.
- Technical and organizational measures applied (or to be applied) to the affected personal data.
- Relevant use of other providers (where applicable).

Second notification - A summary of the incident that caused the breach, including the physical location of the breach and the storage media involved.

- The number of individuals concerned
- The potential consequences and potential adverse effects on those individuals.

- The technical and organizational measures taken to mitigate those potential adverse effects.
- The content of any notification to customers.
- The means of communication used to notify customers.
- The number of customers notified.
- Whether the breach affects individuals in other EU member states.
- Any notification of other data protection authorities.
- If all these details cannot be included in the second notification, a reasoned justification for the further delay.

Customer notification

- The name of the service provider.
- The name and contact details of the data protection officer or other contact point where more information can be obtained.
- A summary of the incident causing the breach.
- The estimated date of the incident.
- The nature and content of the personal data concerned (and in particular whether it included sensitive personal data, financial information, location data, internet log files, web browsing histories, email data or itemized call lists).

- The likely consequences of the breach on the individual concerned (and in particular whether there is a risk of identity theft or fraud, physical harm, distress or damage to reputation).
- Measures taken by the provider to address the breach.
- Measures the individual could take to mitigate any possible adverse effects of the breach.

Appendix 4 Example XML document for SB24-44115 Home Depot Security Breach

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<disclosure>
  <id>SB24-44115</id>
  <organization_name>Home Depot</organization_name>
  <industry_sector>Retail</industry_sector>
  <file_date>Feb 24, 2012</file_date>
  <threat_agent>
    <ident>
      <date></date>
      <type>internal</type>
      <desc>As part of an ongoing investigation, we have
been informed that three HR associates have been arrested on allegations
that include the unlawful use of personal information belonging to
current and former associates and a small number of candidates.</desc>
      <by>HR Associates</by>
    </ident>
    <ident>
      <date></date>
      <type>internal</type>
      <desc>These HR associates were employed by The Home
Depot in positions of trust and therefore had authorized access to your
personal information to perform assigned job duties.
      </desc>
      <by>HR Associates</by>
    </ident>

    These HR associates were employed by The Home Depot in
positions of trust and therefore had authorized access to your personal
information to perform assigned job duties.
  </threat_agent>
  <threat>
    <ident>
      <type>unlawful use of personal information</type>
      <desc>As part of an ongoing investigation, we have
been informed that three HR associates have been arrested on allegations
that include the unlawful use of personal information belonging to
current and former associates and a small number of candidates.</desc>
    </ident>
    <ident>
      <type>possible unlawful use of your personal
information</type>
      <date>February 7, 2011</date>
      <desc>The information that could have been accessed by
the arrested associates includes your name, contact information, social
security number, driver's license number, and any financial account
numbers you may have provided us, and the longest period of employment
for any of the three arrested associates goes back to February 7, 2011.
```

```

</desc>
    </ident>
  </threat>
  <vulnerability>
    <ident>
      <type></type>
      <desc></desc>
    </ident>
  </vulnerability>
  <discovery>
    <ident>
      <date></date>
      <by></by>
      <desc>As part of an ongoing investigation, we have been informed
that three HR associates have been arrested on allegations that include
the unlawful use of personal information belonging to current and former
associates and a small number of candidates.</desc>
    </ident>
  </discovery>
  <investigation>
    <ident>
      <date></date>
      <by></by>
      <desc>As part of an ongoing investigation, we have
been informed that three HR associates have been arrested on allegations
that include the unlawful use of personal information belonging to
current and former associates and a small number of candidates.</desc>
    </ident>
    <ident>
      <date></date>
      <by></by>
      <desc>Our investigation indicates that your
information may have been accessed by one of these three associates for
unlawful purposes.
    </desc>
    </ident>
    <ident>
      <date></date>
      <by>government authorities</by>
      <desc>Because we take this matter very seriously, we
are conducting a thorough internal investigation, and we are working
closely with appropriate government authorities.
    </desc>
    </ident>
  </investigation>
  <impact_assessment>
    <ident>
      <type>possible unlawful use of your personal
information</type>
      <desc>Out of an abundance of caution, we are notifying
you of the possible unlawful use of your personal information.</desc>
    </ident>

```

```
<ident>
  <type>possible unlawful use of your personal
information</type>
  <date>February 7, 2011</date>
  <desc>The information that could have been accessed by
the arrested associates includes your name, contact information, social
security number, driver's license number, and any financial account
numbers you may have provided us, and the longest period of employment
for any of the three arrested associates goes back to February 7, 2011.
</desc>
</ident>
<ident>
  <type>found no evidence </type>
  <date></date>
  <desc>Although we have found no evidence that your
information was inappropriately used at this time, we want to make sure
you can take appropriate steps to help prevent the misuse of your
personal information.
  </desc>
</ident>
<ident>
  <type>open credit card or consumer loan accounts in
your name</type>
  <date></date>
  <desc>The AllClear ID service may be helpful because
one possible misuse of your information would be to open credit card or
consumer loan accounts in your name without your permission.

  </desc>
</ident>
<ident>
  <type>open credit card or consumer loan accounts in
your name</type>
  <date></date>
  <desc>The AllClear ID service may be helpful because
one possible misuse of your information would be to open credit card or
consumer loan accounts in your name without your permission.

  </desc>
</ident>
<ident>
  <type>loss of your credit worthiness</type>
  <date></date>
  <desc>The theft of your identity can lead to the loss
of your credit worthiness and can cause collection agencies to try to
collect debts from you that you did not create.

  </desc>
</ident>
</impact_assessment>
<remediation>
  <ident>
```

```

        <date></date>
        <type>identity protection</type>
        <by>AllClear ID</by>
        <desc>We have arranged for you to receive 12 months of
identity protection from AllClear ID at no cost to you.</desc>
    </ident>
    <ident>
        <date></date>
        <type>credit Monitoring</type>
        <by>AllClear ID</by>
        <desc>AllClear ID offers Credit Monitoring that
delivers secure, actionable Alerts to you by phone.</desc>
    </ident>
    <ident>
        <date></date>
        <type>$1,000,000 Identity Theft Insurance Policy</type>
        <by>AllClear ID Investigations Team</by>
        <desc>This service also includes a $1,000,000 Identity
Theft Insurance Policy, the AllClear ID Investigations Team to assist
you in the event that your information is used fraudulently, and
AllClear ID Resolution Services, if needed, to assist you in restoring
your credit file.</desc>
    </ident>
    <ident>
        <date></date>
        <type>review and monitor relevant account statements
and credit reports.</type>
        <by>you</by>
        <desc>We encourage you to remain vigilant, and to
regularly review and monitor relevant account statements and credit
reports.</desc>
    </ident>
    <ident>
        <date></date>
        <type>report the possible threat to your identity to
local law enforcement</type>
        <by>you</by>
        <desc>If you find any indication of unauthorized
accounts or transactions, you should report the possible threat to your
identity to local law enforcement, your State Attorney General's office,
or the Federal Trade Commission.
</desc>
    </ident>
    <ident>
        <date></date>
        <type>one free credit report</type>
        <by>each of the three national credit bureaus</by>
        <desc>You are entitled to one free credit report
annually from each of the three national credit bureaus.
</desc>
    </ident>
</remediation>
```



```
<other>
  <contact>
    <ident>
      <desc>You may sign up online at enroll.allclearid.com
or by phone by calling 1-877-263-7996.</desc>
    </ident>

  </contact>
  <apology>
</apology>
  <signed>
    <ident>
      <desc>Tonia Horton Senior Director, HR Services </desc>
    </ident>

  </signed>
</other>
</disclosure>
```

Appendix 6-1: Coding Example for Time Identifications

ID	Task	Context	Score	Evidence
sb24-22123	Time Recognition	investigation	1	SF Fire Credit Union completed our investigation on January 1, 2012.
sb24-22123	Time Recognition	detection	1	On the night of December 29, 2011, a laptop used in preparation for the merger of SF Fire Credit Union with Pacifica-Coastside Credit Union was stolen from a parked car in San Francisco.
sb24-22147	Time Recognition	detection	1	When the package arrived at its destination on November 18, 2011, the flash drive was missing.
sb24-22147	Time Recognition	remediation	1	To obtain this credit monitoring report on your account, you must enroll before June 30, 2012.
sb24-22147	Time Recognition	remediation	1	The help line will be staffed from 8 a.m. to 5 p.m. Central Time, Monday through Friday, from now until March 31, 2012.
sb24-22147	Time Recognition	remediation	1	We encourage individuals receiving Ernst & Young LLP's letter dated January 23, 2012, to take the following steps: Order Your Free Credit Report.
sb24-22262	Time Recognition	others	1	The purpose of this letter is to notify you that your personally identifiable information (PII) was recently found in a little-known location on a public web server along with data for a group of employees of the failed IndyMac Bank, F.S.B. (in receivership since July 11, 2008), and its subsidiary, IndyMac Resources, Inc.
sb24-22262	Time Recognition	impact	1	The information posted included name, Social Security Number, birth date, earnings, hire date, and certain other employment-related information for employees from January 1, 1999, to January 1, 2005.
sb24-22302	Time Recognition	impact	1	If you have accessed your Steam account since November 10, 2011 you know that we had a network intrusion.
sb24-22311	Time Recognition	incident	1	On December 31, 2011, a thief(ves) broke into our office.
sb24-22311	Time Recognition	detection	1	The theft was discovered in the early morning hours of January 3, 2012 after the New Years' Eve holiday weekend, and local police authorities were notified at that time.

Appendix 6-2 Coding Example of Logical Reasoning

ID	Task	Context	Score	Evidence
sb24-63669	Logical Reasoning	remediation	1	You should immediately report any unauthorized charges to your card issuer <i>because</i> payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner.
sb24-63675	Logical Reasoning	impact	1	We believe that certain information that you provided to M Securities, such as your name, address, Social Security number, driver's license or identification number, and financial account number may have been stored on this device and could have potentially been affected <i>as a result of</i> the theft.
sb24-63675	Logical Reasoning	impact	1	Please note, at this time, we are not aware of any fraud or misuse of your information <i>as a result of</i> this incident.
sb24-63841	Logical Reasoning	threat	1	Instead it poses an operational risk to health systems in <i>that it can result in</i> patients being turned away due to an inability to provide care as a result of not having immediate access to records.
sb24-63841	Logical Reasoning	impact	1	<i>Nevertheless, as a result of</i> the attack, we were temporarily denied access to certain portions of our computer system, and we regret any delays or rescheduling of appointments that may have resulted from this incident.
sb24-63841	Logical Reasoning	impact	1	<i>Because</i> the attack targeted the entire system, we were temporarily denied access to both internal clinic information and patient data including names, addresses, phone numbers and billing and insurance information.
sb24-63841	Logical Reasoning	impact	1	However, there was a delay in gaining access to certain internal clinic information which, in conjunction with the need to notify appropriate law enforcement authorities, <i>limits our ability to fully explain</i> what happened until this time.
sb24-63841	Logical Reasoning	remediation	1	I <i>conclude</i> by noting that <i>due to</i> the rapid increase in such incidents across the nation and the likelihood of similar attacks in the future, we have implemented additional steps to enhance the security of our computer systems, including reviewing our security processes, software, and hardware, in an effort to help reduce the likelihood of a similar attack in the future and to help minimize any delays in service which might occur in the event of such a future attack.
sb24-63841	Logical Reasoning	remediation	1	While we cannot guarantee that similar such attacks will not occur in the future, what we can do is once again apologize for any delays, rescheduling, or other inconvenience that <i>may have resulted</i> from this incident.

Appendix 7 Summary of State level Data Security Laws

Arizona	<u>Ariz. Rev. Stat. § 18-105</u>	State budget units and state agencies	Establishes a statewide information security and privacy office. Provides that the office serve as the strategic planning, facilitation and coordination office for information technology security in the state. Individual budget units continue to maintain operational responsibility for information technology security. Provides for the appointment of a statewide chief information security officer to manage the statewide information security and privacy office. Requires the office to direct security and privacy compliance reviews, identify and mitigate security and privacy risks, monitor compliance with policies and standards, and coordinate training programs.
California	<u>Calif. Govt. Code § 11549.3 et seq., Calif. Govt. Code § 8592.30-8592.45</u>	State agencies.	Comply with information security program developed by the Chief of the Office of Information Security, as specified/detailed in statute , including conducting an annual independent security assessment. Requires each state agency to implement cybersecurity strategy incident response standards to secure its critical infrastructure controls and critical infrastructure information.
Colorado	<u>C.R.S. §§ 24-37.5-401 et seq.</u>	Public agencies, institutions of higher education	The chief information security officer shall: (a) Develop and update information security policies, standards, and guidelines for public agencies; (b) Promulgate rules pursuant to article 4 of this title containing information security policies, standards, and guidelines; (c) Ensure the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by public agencies pursuant to <i>section 24-37.5-404</i> ; (d) Direct information security audits and assessments in public agencies in order to ensure program compliance and adjustments. Establishes the Colorado Cybersecurity Council and provides for coordination of missions related to homeland security and cybersecurity.
Connecticut	<u>C.G.S. § 4e-70</u>	Any state agency with a department head and any state agency disclosing confidential information to a contractor	Implement and maintain a comprehensive data-security program for the protection of confidential information. The Secretary of the Office of Policy and Management, or the secretary's designee, may require additional protections or alternate measures of security assurance when

		pursuant to a written agreement with such contractor for the provision of goods or services for the state.	warranted.
Florida	<u>Fla. Stat. § 282.318,</u> <u>Fla. Stat. § 20.61</u>	State agencies.	Comply with the statewide information technology security standards and processes developed by the Agency for State Technology as specified/detailed in statute , including conducting and updating a comprehensive risk assessment every three years, creating an incident response team and reporting process, and providing security and cybersecurity awareness training for all state agency employees.
Georgia	<u>Georgia Code § 50-25-4</u>	Agencies	The Georgia Technology Authority shall have the following powers (21) To establish technology security standards and services to be used by all agencies; (22) To conduct technology audits of all agencies;
Indiana	<u>Ind. Code § 4-13.1-2-2</u>	State agencies	The Office Of Technology shall: (9) Review projects, architecture, security, staffing, and expenditures. (10) Develop and maintain policies, procedures, and guidelines for the effective and secure use of information technology in state government. (11) Advise the state personnel department on guidelines for information technology staff for state agencies. (12) Conduct periodic management reviews of information technology activities within state agencies upon request.
Kentucky	<u>K.R.S. § 42-724</u> <u>K.R.S. § 61.932(1)</u>	Public agencies and nonaffiliated third parties.	An agency or nonaffiliated third party that maintains or otherwise possesses personal information, regardless of the form in which the personal information is maintained, shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches. Reasonable security and breach investigation procedures and practices established and implemented by organizational units of the executive branch of state government shall be in accordance with relevant enterprise policies established by the Commonwealth Office of Technology.
Maryland	<u>Md. State Govt. Code §§ 10-1301 to -</u>	An executive agency, a department, a board, a	Implement and maintain a written information security policy and reasonable security procedures and practices that are appropriate to the nature of the personal

	<u>1304</u>	commission, an authority, a public institution of higher education, a unit or an instrumentality of the State; or a county, municipality, bi-county, regional, or multicounty agency, county board of education, public corporation or authority, or any other political subdivision of the State.	information collected and the nature of the unit and its operations. Require, by written contract or agreement, that third parties implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information disclosed to the nonaffiliated third party.
Massachusetts	Mass. Gen. Laws <u>Ch. 93H § 2(c)</u>	The legislative branch, the judicial branch, the attorney general, the state secretary, the state treasurer and the state auditor.	Adopt rules or regulations designed to safeguard the personal information of residents of the commonwealth for their respective departments and shall take into account the size, scope and type of services provided by their departments, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.
Minnesota	Minn. Stat. <u>§ 16E.03</u>	State agencies in the executive branch of state government, including the Minnesota Office of Higher Education, but not the Minnesota State Colleges and Universities.	Provides that the chief information officer (CIO) shall establish and enforce standards and ensure acquisition of hardware and software necessary to protect data and systems in state agency networks connected to the Internet. Further provides that the CIO shall establish cyber security policies, guidelines, and standards and install and administer state data security systems on the state's computer facilities consistent with policies, guidelines, standards, and state law to ensure the integrity of computer-based and other data and to ensure applicable limitations on access to data.
Montana	<u>Mont. Code § 2-6-1502</u>	Each state agency that maintains personal information.	Develop procedures, as specified/detailed in statute , to protect personal information while enabling the state agency to use personal information as necessary for the performance of its duties under federal or state law.
New York	<u>New York State Tech. Law § 103</u>	State agencies.	Provides for the office of information technology services to advise and assist state agencies in developing policies, plans and programs for improving the statewide coordination, administration, security, confidentiality, program effectiveness, acquisition and deployment of technology. Also authorizes the office to perform technology reviews and make recommendations for improving management and program effectiveness pertaining to technology; and to review and coordinate the purchase of technology by state agencies. Requires that, where applicable, the review should include but not be limited to: assessing consistency with the statewide strategic technology plan and agency technology plan; statewide technology standards; the safeguarding of information privacy; security of confidential records;

			and proper dissemination of public information. Also authorizes the office to establish statewide technology policies, including but not limited to preferred technology standards and security, including statewide policies, standards, programs, and services relating to the security of state government networks and geographic information systems. Also provides for the protection of the state government's cyber security infrastructure, including, but not limited to, the identification and mitigation of vulnerabilities, deterring and responding to cyber events, and promoting cyber security awareness within the state.
North Carolina	<u>N.C. Gen. Stat. § 147-33.110 to -33.112</u>	State agencies.	The state Chief Information Officer shall establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the state's distributed information technology assets, including communications and encryption technologies. The state CIO shall review and revise the security standards annually. As part of this function, the state Chief Information Officer shall review periodically existing security standards and practices in place among the various state agencies to determine whether those standards and practices meet statewide security and encryption requirements. The state Chief Information Officer may assume the direct responsibility of providing for the information technology security of any State agency that fails to adhere to security standards adopted under this Article.
Ohio	<u>Ohio Rev. Code § 125.18</u>	State agencies	Provides that the chief information officer shall establish policies and procedures for the security of personal information that is maintained and destroyed by state agencies. Provides for a chief information security officer (CISO) who is responsible for the implementation of such policies and procedures. Also provides for the CISO to assist agencies with IT security strategic plans and to review those plans.
Oklahoma	<u>62 Okl. St. § 34.32</u>	Each state agency that has an information technology system.	Conduct an annual information security risk assessment to identify vulnerabilities associated with the information system. The final information security risk assessment report shall identify, prioritize, and document information security vulnerabilities for each of the state agencies assessed. Failure to comply with the requirements of this subsection may result in funding being withheld from the agency. State agencies shall use either the standard security risk assessment created by the Information Services Division or a third-party risk assessment meeting the ISO/IEC 17799 standards and using the National Institute of Standards and Technology Special Publication 800-30 (NIST SP800-30) process and approved by the Information Services Division.
Oregon	<u>ORS § 182.122,</u> <u>2016 Ore. Laws Chap.</u>	State agencies	Provides for the Oregon Department of Administrative Services, in its sole discretion, to (a) Review and verify the security of information systems operated by or on behalf of agencies;

	<u>110</u>		<p>(b) Monitor state network traffic to identify and react to security threats; and</p> <p>(c) Conduct vulnerability assessments of agency information systems for the purpose of evaluating and responding to the susceptibility of information systems to attack, disruption or any other event that threatens the availability, integrity or confidentiality of information systems or the information stored in information systems.</p>
South Carolina	<u>2015 H.B. 3701</u> (Budget bill)	All state agencies.	<p>Adopt and implement cyber security policies, guidelines and standards developed by the Department of Administration. The department may conduct audits on state agencies as necessary to monitor compliance.</p> <p>Upon request, public institutions of higher learning, technical colleges, political subdivisions, and quasi-governmental bodies shall submit sufficient evidence that their cyber security policies, guidelines and standards meet or exceed those adopted and implemented by the department. Exempts judicial and legislative branches.</p>
Texas	<u>Tex. Govt. Code § 2054.0286</u>	State agencies	<p>Provides for employment of a statewide data coordinator to improve the control and security of information collected by state agencies;</p> <p>Requires the statewide data coordinator to develop and implement best practices among state agencies to improve information management and analysis to increase information security.</p>
Utah	<u>Utah Code § 63F-2-102</u>		Creates a data security management council, which shall review existing state government data security policies, assess ongoing risks, notify state and local entities of new risks, coordinate breach simulation exercises, develop data security best practices recommendations for state government. Provides for hiring and training of a chief information security officer for each government entity.
Virginia	<u>Va. Code § 2.2-603</u> <u>Va. Code § 2.2-2009</u>	Every agency and department in the executive branch of state government, including those appointed by their respective boards or the Board of Education	<p>Every agency and department is responsible for securing the electronic data held by his agency or department and shall comply with the requirements of the commonwealth's information technology security and risk-management program as set forth in § <u>2.2-2009</u>, and shall report all known incidents that threaten data security.</p> <p>The CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information. Such policies, procedures, and standards will apply to the commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education. The CIO shall also develop policies, procedures, and standards that shall address the</p>

			scope of security audits and the frequency of such security audits.
Washington	<u>RCW 43.105.054</u> <u>RCW 43.105.020,</u> <u>RCW § 43.105.215</u>	State agencies (certain provisions also apply to institutions of higher education the legislature, and the judiciary)	Requires the Consolidated Technology Services Agency to establish establish security standards and policies to ensure the confidentiality, availability, and integrity of the information transacted, stored, or processed in the state's information technology systems and infrastructure. Also provides for implementing a process for detecting, reporting, and responding to security incidents. The director shall appoint a state chief information security officer. Requires each state agency, institution of higher education, the legislature, and the judiciary to develop an information technology security program that adheres to the office's security standards and policies. Requires each state agency to review and update its program annually and certify to the office that its program is in compliance with the office's security standards and policies. Requires state agencies to obtain an independent compliance audit at least once every three years.
West Virginia	<u>W.V. Code § 5A-6-4a</u>	Every agency and department.	The Chief Technology Officer is authorized to develop policies, procedures, standards and legislative rules that identify and require the adoption of practices to safeguard information systems, data and communications infrastructures. Provides for annual security audits of all executive branch agencies regarding the protection of government databases and data communications.
Wyoming	<u>Wyo. Stat. § 9-21-101</u>	Every agency, department, board, commission, council, institution, separate operating agency or any other operating unit of the executive branch of state government.	Requires every agency to adopt, enforce and maintain a policy regarding the collection, access, security and use of data. The policy shall, at a minimum, comply with applicable federal and state law, adhere to standards set by the state chief information officer and include the following: (i) An inventory and description of all data required of, collected or stored by an agency; (ii) Authorization and authentication mechanisms for accessing the data; (iii) Administrative, physical and logical security safeguards, including employee training and data encryption; (iv) Privacy and security compliance standards; (v) Processes for identification of and response to data security incidents, including breach notification and mitigation procedures; (vi) In accordance with existing law, processes for the destruction and communication of data.