INFORMATION THEFT WITHIN DIFFERENT ORGANIZATIONAL TYPES: A RATIONAL CHOICE ANALYSIS

By

JEONG HYUN KIM

A dissertation submitted to the

Graduate School - Newark

Rutgers, the State University of New Jersey

In partial fulfillment of requirements

For the degree of

Doctor of Philosophy

Graduate Program in Criminal Justice

Written under the direction of

Dr. Ronald V. Clarke

And approved by

Dr. Ronald V. Clarke

Dr. Norman Samuels

Dr. Andres F. Rengifo

Dr. Graeme R. Newman (Outside Reader)

Newark, New Jersey

May, 2015

ABSTRACT OF THE DISSERTATION

Information Theft within Different Organizational Types: A Rational Choice Analysis

By JEONG HYUN KIM

Dissertation Chair: Ronald V. Clarke

As the world becomes more connected through technology and the internet, words "identity theft" and "data breach" become part of everyday conversation, signaling the rise of those incidents. Major sources of identity theft and data breach from organizations include hacking, insider theft, stolen or lost IT devices, data exposure from websites, information exposure from mailing errors, and dumped documents. The most direct of these sources are hacking and insider theft. The increasing availability of information unfortunately comes with an increased risk of its exploitation. The goals of this dissertation are to determine which organizations are vulnerable to outside hacking and insider theft, to examine how the nature of a theft and the type of an organization influence the time needed to detect the crime, and to investigate whether or not these incidents experience seasonal variation.

Guided by Rational Choice theory, this dissertation focuses on incidents of hacking and insider theft that occur within four types of organizations: business, education, healthcare/medical and government. This dissertation consists of two parts: analyses of information thefts at four types of organizations and IT security incidents at 24 U.S. federal agencies. An analysis of data collected from non-profit organizations, the Open Security Foundation and the Identity Theft Resource Center from 2007 to 2013 shows that the total number of reported information theft incidents is 1,895, among which hacking incidents make up 1,114 cases, and insider thefts comprise 781 cases. Additionally, U.S. federal agencies' IT security incidents were analyzed using the White House reports of 2012 and 2013. These cases are analyzed by the method of theft, type and size of the organization in question, and the detection period of each incident. The "SCAREM" model are used to analyze the characteristics of those incidents. Incidents of seasonal time variances are examined as well.

Findings indicate that the theft rates of hacking and insider incidents are likely to be higher in larger organizations. Insider theft typically goes unnoticed longer than any other instance of cyber infiltration within the majority of organizations.

U.S. federal agencies show a positive correlation between organization size and the occurrences of IT security incidents. Occurrences of IT security incidents are unequally distributed among federal agencies. Incidents of mis-handled information show seasonal variations. Analyses with the concepts of "Risky organizations" indicate that larger federal agencies except NASA show more vulnerabilities to IT security incidents.

This dissertation applies situational crime prevention strategies that may reduce the opportunities for offenders. Maintaining constant IT monitoring practices and trainings for protecting valuable assets, information and data are recommended. A more comprehensive database logging incidents of information theft and data breaches is necessary.

ACKNOWLEDGEMENTS

The long and lonely journey I embarked on several years ago is over. At the beginning of it, I questioned the possibility of achieving my goal. Fortunately, my dream has become a reality. Now having completed this goal, I realize that my fate directs me take on new goals that will continue my life’s adventure.

This dissertation would not have been possible without the support, guidance, patience and love of many people. First, I would like to express my heartfelt appreciation to my dissertation chair, Dr. Ronald V. Clarke. I am deeply grateful for his immeasurable support and advice for my dissertation and academic life. I would also like to thank the members of my dissertation committee: Dr. Norman Samuels, Dr. Andres F. Rengifo, and Dr. Graeme Newman for their invaluable mentoring and guidance. I must thank Dr. James O. Finckenauer and Dr. Ko-Lin Chin for their warm encouragement. Furthermore sincere gratitude must go to my friends, professors, and staff at the Rutgers School of Criminal Justice. To my old friends and colleagues in Seoul, who could always cheer me up through this unusual journey, I say, “Thank you.” My special thanks also goes to Lynnette Krueger for her never-ending encouragement and thorough proof reading.

I must thank my lovely family, my wife, Sook Hee Choi, and my daughters, Min Jee and Min Cheong for their endless patience and warm support. Without their love, I would not have been able to complete my doctoral work and this dissertation. Our family dinners and conversation throughout these years of study have always kept me grounded, lifted my spirits and inspired me. I must also express my deep thankfulness to my mother-in-law, Yang Soon Cho and my late father-in-law, Suk Hwan Choi. Their

tremendous and generous support has made this journey successful far away from my home. I also thank my sisters and brother in Seoul for their support.

Finally I would like to dedicate this dissertation to my dearly departed parents: Ock Gyung Jee and Si Chul Kim. “Mother and father, I did it. Rest in peace.”

TABLE OF CONTENTS

Appendices

LISTS OF TABLES

LIST OF TABLES

LISTS OF FIGURES

SUMMARY

Objectives

The words “identity theft” and “data breach” are frequently used in contemporary media. This dissertation uses the term “information theft” to describe outsider hacking and insider theft occurring within organizations in four fields: business, education, healthcare/medical and government. The goals of this dissertation are to determine which organizations are vulnerable to outside hacking and insider theft, to examine how the nature of a theft and the type of a target influence the time needed to discover the crime, and to investigate whether or not these incidents experience seasonal variation.

Because offenders tend to plan carefully before committing a crime, this research hypothesizes that they decide what kind of organization they will target based largely on environmental factors, which they review before attempting an infiltration. To extrapolate that hypothesis, this dissertation uses Rational Choice Theory and Situational Crime Prevention Theory as theoretical frameworks. Rational Choice Theory dictates that criminals commit crimes after weighing the benefits of the crime against the cost of being caught and punished (Becker, 1968; Cornish and Clarke, 1986, 2000). This theory is well suited to explaining offenders’ decision process, especially it is recognized that the decision process is also influenced by “bounded rationality.”

This dissertation consists of two parts. Part One explores the types of information in the aforementioned four types of organizations, characteristics of organizations which are vulnerable to information theft, detection time period, and seasonal variation of information theft. Additionally, the SCAREM model is used to explain the characteristics

of information theft.

Part Two examines features of IT security incidents reported in 24 U.S. federal agencies, characteristics of agencies which are vulnerable to IT security incidents, and seasonal variation of IT security incidents. The “Risky organizations” model is adopted to explore vulnerable agencies from IT security incidents.

Part One

Incident data of information theft was collected from the databases of the “Open Security Foundation” and the “Identity Theft Resource Center” from 2007 to 2013. A total of 1,980 cases of information theft were identified, broken down in Table A:

Table A: Total Incidents of Information Theft Identified in Four Types of Organizations.

	Business	Education	Healthcare/ Medical	Government	Total
Hacking	758	171	61	124	1,114
Insider theft	412	22	196	151	781
Total	1,170	193	257	275	1,895

The unit of analysis is an incident of information theft reported in four types of organizations. The dependent variable is the rate of information theft. The information theft rate was calculated by dividing the total number of incidents by the total number of organizations within each organizational category, and multiplying the quotient by 100. The independent variables are the type of organization, the size of the organization measured by employees, and the time period between the incident and its detection.

The sub-category "Business" includes banking, insurance, finance, information, manufacturing, restaurant, retail, hotel, service, and management industries. "Education" includes colleges and universities. "Healthcare/Medical" encapsulates hospitals, clinics and healthcare offices. Finally, "Government" includes governments and agencies at the local, city, state and federal level.

Guided by Rational Choice Theory, research questions, hypotheses and the findings are outlined below Table B.

Table B: Research Questions, Hypotheses and Findings for Four Types of Organizations.

Research Questions	Hypotheses		Findings	
RQ 1: What kinds of organizations are vulnerable to what kinds of information theft? RQ 2: Does the time taken to detect information theft vary with the nature of the theft and organizations? RQ 3: Does information theft show any seasonal variation in organizations?	H1	Hacking incidents are more likely to occur at smaller organizations.	- Confirmed: Business & Medical. - Not confirmed: Educational & Governmental.	
	H2	Insider theft incidents are more likely to occur at larger organizations.	- Confirmed: Business, Medical & Governmental. - Not confirmed: Educational.	
	H3	Governmental organizations will likely experience higher rates of information theft.	Confirmed.	
	H4	Insider theft incidents will take a longer time to detect.	Confirmed.	
	H5	Governmental organizations will detect the information theft more quickly.	Not confirmed.	
	H6	Information theft incidents are not likely to show seasonal variation.	Hacking	- Confirmed: Business, medical & governmental. - Not confirmed: Educational.
			Insider theft	- Confirmed: Business, medical & governmental. - Excluded: Educational.

For analysis of the characteristics of information theft, the SCAREM model is used. This is a model for identifying "the elements of the information system itself that are conducive to crime with the acronym SCAREM: Stealth, Challenge, Anonymity, Reconnaissance, Escape and Multiplicity" (Newman and Clarke, 2003, p.61). For the SCAREM model of hacking, method of offense is conceptualized as "Stealth." Preparedness for a crime is conceptualized as "Reconnaissance." Detection period is conceptualized as "Escape." Secondary offenses are conceptualized as "Multiplicity." "Challenge" and "Anonymity" are not operationalized as the data for this research is not available.

Regarding the SCAREM model for insider theft rates, the method by which information was stolen is conceptualized as "Challenge." "Anonymity" is conceptualized by status of insiders. The concepts "Reconnaissance," "Escape," and "Multiplicity" are conceptualized in the same way as hacking incidents in the SCAREM model.

Part One Findings (see Table B)

Hacking incidents most commonly afflict small businesses and medical centers, while insider theft most commonly afflicts large businesses and medical organizations. Educational institutions experience hacking more frequently when they are large, while insider thefts are more commonplace in smaller schools. State-level governments experience more hacking incidents compared to other types of governments (*H1 & H2*). Governments are more likely to be targets by hackers and insider offenders (*H3*). Insider theft takes longer to detect (*H4*). Governments detect hacking incidents quickly but statistical analysis does not support this. Insider theft at medical organizations takes longer to detect (*H5*). Hacking and insider theft incidents in business, medical and governmental organizations do not show seasonal variation (*H6*).

The application of the SCAREM model to hacking and insider theft is shown in Table C. For the SCAREM model of hacking, hacking rates are found to be positively related to the attribute of “Reconnaissance.” This indicates that the more preparation is involved in hacking incidents, the more likely they will be successful. Hacking rates are inversely related to the attributes of “Stealth,” and “Escape.” These mean that organizations with higher rates of hackings are vulnerable to the attacks in lower levels of hacking skills, and higher rates of hackings correspond directly with a lower level of IT security management, a longer detection period. Lastly, the concept of “Multiplicity” which shown an inverse relationship means that organizations with higher rates of hackings will show less frequency of secondary incidents resulting from the stolen data.

Table C: Spearman’s Rho Correlation Analysis for the SCAREM Model.

	Hacking Rate
Stealth	-.08**
Reconnaissance	.13**
Escape	-.11**
Multiplicity	-.19**

	Insider Theft Rate
Challenge	-.1**
Anonymity	
Reconnaissance	
Escape	.2**
Multiplicity	-.11**

** $p < .01$, * $p < .05$.

Regarding the SCAREM model for insider theft rates, insider theft rates are positively related to the concept of “Escape,” meaning the more an organization suffers insider theft, the longer it takes to discover those incidents. Concepts of “Challenge,” and “Multiplicity” are inversely related to insider theft rates. These findings indicate that information may be accessed with limited restrictions and insider thefts are coming from more availability of basic levels of information.

Part Two

In Part Two, federal agencies are examined more closely. This is because mass media pays the most attention to federal agencies and those agencies are popular targets from international hackers.

IT security incidents at 24 federal agencies occurring from 2012 to 2013 were examined. Data was collected from a source of the U.S. Computer Emergency Readiness Team (US-CERT). IT security incidents are categorized by US-CERT as one of the following: unauthorized access, equipment lost/stolen, denial of service, malicious code, improper usage, policy violation, social engineering, suspicious network activity, non-cyber type incident, and other incidents.

For the analysis of seasonal variations in non-cybercrime IT security incidents, the Department of Veterans Affairs is selected. The VA Department maintains an extensive record of IT security incidents because the Department is required to report the incidents to Congress.

Three environmental factors have been developed in this dissertation for analyzing IT security issues in federal agencies: (1) management factor: Federal Information Security Management Act of 2002 (FISMA) compliance scores, IT security personnel rate, and IT security budget rate; (2) opportunity factor: Number of employees, IT budget rate, open datasets, and number of related branches; and (3) incident type: Cybercrime type IT security incidents, non-cybercrime type IT security incidents, and unknown type IT security incidents.

As a dependent variable, the IT security incident rate is calculated by dividing the average number of incidents at the respective agencies by the total budget at each agency. Guided by Rational Choice Theory, research questions, hypotheses and their findings are outlined in Table D.

Table D: Research Questions, Hypotheses and Findings for Federal IT Security Incidents.

Research Questions	Hypotheses		Findings
RQ 4: Are IT security incidents equally distributed among federal agencies? RQ 5: What kinds of federal agencies are vulnerable to what kinds of IT security incidents? RQ 6: Do IT security incidents show seasonal variation?	H7	IT security incidents are more likely to be unequally distributed among federal agencies.	Confirmed.
	H8	Cybercrime-type IT security incidents are more likely to occur at smaller federal agencies.	Not confirmed.
	H9	Non-cybercrime type IT security incidents are more likely to occur at larger federal agencies.	Confirmed.
	H10	Non-cybercrime type IT security incidents are not likely to show seasonal variation.	- Not confirmed: Mis-handled information. - Confirmed: Stolen/missing IT devices.

Eck, Clarke, and Guerette (2007) introduced a concept of “Risky Facilities Analyses,” and Clarke and Newman (2006) developed a model of “EVIL DONE” for identifying international terrorists’ target features. Based on these two models, this dissertation develops the metrics of “Risky organizations” concept for identifying vulnerable organizations from the IT security incidents in 24 federal agencies. This research uses the incident rate, numbers of incident, total budget, employees, IT budget rate for an opportunity factor. Compliance scores, IT security personnel rate, and IT security budget rate are used for a vulnerability factor.

Part Two Findings (see Table D)

In the bivariate analysis testing the relationship between IT security incident rates and three environmental factors, IT security incidents are found to be unequally distributed among 24 federal agencies (*H7*). Employee numbers in opportunity factors are positively related to cyber-crime type and non-cybercrime type incidents (*H8 & H9*), meaning that larger organizations produce more reports of IT security incidents. With the data analysis from the VA Department, seasonal variation is found in incidents of mishandled data and information. Incidents of stolen/lost IT devices show no seasonal variation (*H10*).

With the metrics of “Risky organizations,” the Department of Health and Human Services is found to be the top ranked target among other federal agencies (See Table F).

Table F: Top Five Federal Agencies’ Scores for “Risky Organizations” Metrics

Variable / Dept.	Opportunities						Vulnerabilities			Total Scores
	Incident Rates	Incidents	Budget	Employees	IT Budget Rate	Related Branch	Compliance Scores	IT Personnel Rate	IT Security Budget Rate	
HHS		4	5			5	3		3	20
NASA	5	3			3				5	16
VA		5		4				2	4	15
USDA			1			4	5	4		14
DOD*			3	5		3				11

*Compliances scores are not available at the DOD.

Conclusions

The data used in Part One has several internal limitations. First, the data used are not official data compiled by law enforcement organizations. Second, public media resources do not cover every incident of information theft across the country. Information theft is usually not a top priority when compared to violent crime, so the public remains ignorant of the scale of damage it causes. Third, direct surveys on information theft typically yield a low rate of responses. Therefore, public media are the inevitable and viable source for this information theft research.

Based on the findings, constant monitoring of information management shall be a priority security measure, as well as training for enhancing the ethics of keeping information and data. Proper and timely prevention measures in organizations can be effective pursuant to diagnosing vulnerabilities in IT security systems. Regular, comprehensive analysis for the vulnerabilities in an organization’s IT system is a necessary measure. Following the discussion of information theft, this dissertation offers 25 metrics originally based on Situational Crime Prevention Theory which may reduce the opportunities for information theft, focusing on situational factors.

A more comprehensive database logging incidents of information theft and data breaches is necessary. Exploring the processes how information offenders and criminal cells dispose of stolen data and information will be a follow-up research for the information theft study.

CHAPTER 1: Introduction

1. 1. Problem Statement

Americans share their identification with public and private organizations alike for various purposes. Those organizations handle various types of information collected from or provided by citizens, and produce their own information and data based on their collective goals.

Web applications, mobile devices, point-of-sale devices, and medical devices are used daily for the rapid, convenient services they offer. Despite the benefit of these devices, the information they contain can be exposed to people with criminal intentions. By 2015, one trillion devices will be connected to the internet (King, 2012), making cybercrime an inescapable threat.

Businesses and governments are now considering the use of “Big Data” for “powerful analytic capabilities” and they are “connecting data from different sources, finding patterns and generating new insights (World Economic Forum, 2012, p.7).” As the availability of data and information grows, the opportunity to exploit it increases. Perpetrators of identity theft and data breach can be family members, close friends, political enemies, or employees of a victim, or simply hackers curious about the IT security system of businesses. On occasion, data breaches are committed unwittingly from the inside of an organization.

Law enforcement agencies tend to focus on offenses of a more violent, visible nature than identity theft and data breach, leaving cyber criminals relatively free to do as they please. There is no national level database on identity theft or data breach in the United States. However, the Federal Trade Commission, FBI, and local law enforcement agencies are receiving complaints and crime reports regarding personally identifiable information from victims. These cases may be under-reported as a result of authorities' focus on more violent crime.

There are several different types of identity theft and data breach, across several types of organizations. Data breaches are assessed first on the basis of whether or not they were done with intent. In the scope of intentional purpose, there is hacking and insider theft. In the scope of unintentional purpose, there are cases of stolen or lost IT devices and documents, data exposure from a website or internet search, information exposure from mailing errors, or an instance of dumped documents. The research portion of this dissertation explores the patterns of identity theft and data breaches in the context of each organizational type. For clearing the definition of "information" theft in this research, "information" includes personal and proprietary data.

Current studies include whole patterns of identity theft and data breach in the scope of intentional and unintentional purposes. For a more accurate understanding, this research is focused on information theft perpetrated with intent. There is almost no research to explore how many data breaches end in theft and eventual fraud. Simple addition of data breach or identity theft cases which target organizations may not yield a lasting solution for organizations or individuals. Further, even while focusing on cases of hacking and insider theft, this research bears no indication as to how many of those cases result in fraud committed with the data stolen in those instances.

For the prevention of information theft in contemporary society, this research will explore the feasibility of the "situational crime prevention" approach (Clarke, 1997). The effectiveness of awareness education on the individual level may be limited, as offenders are practically invisible, or are handling personal or monetary information. Systematic prevention measures in organizations may work more effectively, after a diagnosis of where their vulnerabilities lie.

1.2. Dissertation Outline

Chapter One introduces the problems and issues of information theft, outlines the following chapters, and defines data and information. This chapter explains crimes related to information and the terms ‘identity theft’ and ‘data breach.’ This research focuses on thefts of data and information. By combining the definitions of identity theft and data breach, the term ‘information theft’ is adopted for this dissertation.

Chapter Two summarizes the general scope of information theft, introducing the two scopes: insider theft and outsider hacking; the methods of information theft: information theft in business, education, healthcare, and government; laws related to handling identity theft and data breach, and research issues in the study of information theft.

Chapter Three provides the theoretical frameworks of Rational Choice Theory for explaining the characteristics of information theft. The perspective of Situational Crime Prevention Theory is adopted to develop policy implementations. It is hypothesized that certain types of organizations appeal to hackers and insiders differently depending on certain criteria. The “SCAREM” model was developed to explain the characteristics of offenses in e-commerce, and is used in this research to explain the characteristics of information theft. Reports of information theft are also tested for seasonal variation.

Chapter Four explains the research design of this dissertation. Based on the Rational Choice and Situational Crime Prevention theories, research questions and hypotheses are developed for examining the environmental factors of information theft. The unit of analysis is the amount of information thefts. The dependent variable is the rate of hacking and insider theft. Incident rates were calculated by dividing reported incidents at each industrial sector by total firms per those sectors. Independent variables are types of organizations, employee numbers, and detection time periods. Data for this research is collected from: the Open Security Foundation and Identity Theft Resource Center. 1,895 cases are collected in total. Among them, hacking incidents account for 1,114 cases and insider theft for 781 cases.

Chapter Five explores the basic characteristics of information theft in the four types of organizations. In business, larger business and medical organizations experience insider theft more frequently than hacking incidents. Incident detection time was found to vary between types of incidents. In education, while hacking incidents occur more often at large schools. In state governments, hacking incidents and insider theft were both found most common. Available statistics reveal no seasonal variation in hackings that target businesses. There are seasonal variations for hacking incidents targeting educational institutions, however. Hacking rates are positively related to SCAREM’s element “Reconnaissance” and inversely related to the elements “Stealth,” “Escape” and “Multiplicity.” Insider theft rates are inversely related to “Challenge,” “Multiplicity” and positively related to “Escape.”

Chapter Six analyzed IT security incidents beyond information theft in 24 federal agencies. IT security incidents include criminal offenses and human mistakes in managing data and information. The unit of analysis in this chapter is the number of IT security incidents. The dependent variable is the IT security incident rate, measured by dividing the number of incidents by the total budget at each federal agency. The independent variables are FISMA compliance scores, IT security personnel rates, IT security budget rates, employees, IT budget rates, related branches, cybercrime type IT security incidents, non-cybercrime type IT security incidents, and unknown type of IT security incidents.

The IT security incident rate shares a positive relationship with the IT budget rate and cybercrime type incidents. The FISMA compliance scores were found positively related to the IT security personnel rate and IT security budget rate. The number of employees and related branch offices show a positive relationship with cybercrime type incidents and non-cybercrime type incidents.

In the bivariate analyses, IT security incident rates were found positively related to incidents of improper usage, malicious code, and social engineering. Average compliance scores and IT security personnel rates show no relationship with any type of IT security incident. Number of employees is positively related to most IT security incidents. A “Risky organizations” model, based on the models of “Risky facilities,” and “EVIL DONE,” is used to explain the processes of target selection that hackers use for federal agencies. The HHS, NASA, VA, USDA and DOD are identified as top five “Risky organizations” by this model’s analysis.

Chapter Seven describes non-cybercrime type IT security incidents reported by the Department of Veterans Affairs from 2011-2014. Non-cybercrime type IT security incidents are reported as increasing from 2011-2014. This research finds that mis-handled

IT security incidents show seasonal variations. However, stolen/lost IT devices incidents show no seasonal variations at the VA Department.

Chapter Eight summarizes the findings made by this research. Research and data limitations and possible policy implications are addressed as well. This chapter suggests possible methods of information theft prevention. In-house training sessions for employees may help protect data and information, but comprehensive, constant analyses for vulnerabilities in IT management systems prove more effective, and are recommended. Constant, routine monitoring of IT management systems is necessary. This research develops several techniques for information theft reduction based on the 25 technique model created by Newman and Clarke (2003).

1. 3. Definitions of Data, Information and Information Theft

For the purposes of this dissertation, information is defined as “data plus meaning” (Checkl and Scholes, 1990, p.303) or more specifically, “data that has been processed into a form that is meaningful to the recipient (Davis and Olson, 1985, p.200),” while data is meant as “raw material that is processed and refined to generate information (Silver and Silver, 1989, p.6, as cited by Floridi, 2005, p.353).” There is an estimated 2.2 zettabytes of information worldwide for businesses alone, the equivalent of a 374 mile tall stack of paper (Symantec, 2012, p.4). Small and mid-size businesses usually maintain about 563 terabytes of data, while an enterprise typically holds 100,000 terabytes. According to the Symantec report (2012, p.5), worldwide spending (access, storage, compliance, and security) of business information is about 1.1 trillion dollars. Despite these expenses, about one-third of all stored data has minimal to no security, and only half of the information accumulated by businesses is property protected (Mearian, 2011).

According to Newman and Clarke (2003), information is broken into four categories within e-commerce: Intellectual property, intelligence, systems, and services (See Table 1).

Table 1: Information, crimes and targeted product of e-commerce

Category	Crime	Target
Intellectual property	Video piracy, software piracy, copyright violation, counterfeiting	Software, CDs, videos, music
Intelligence	Industrial espionage, extortion and blackmail, credit card fraud, accounting fraud, identity theft, aiding and abetting crime.	Proprietary information, business plans and formulas, databases of credit and personal information, accounting records, credit card users, newsgroup users.
Systems	Vandalism, terrorism, electronic funds transfer fraud, hacking, denial of service, account ting fraud	Bank accounts, websites, databases, accounting records.
Services	Theft of telephone services, electronic funds transfer fraud, cross-border crime, denial of service, cloning of cellar phones and phone cards, credit card fraud, stalking, harassment, money laundering, investment fraud, telemarketing fraud, gambling, tax evasion, criminal conspiracy	Cell phones, phone cards, bank accounts, credit cards, Internet users, personal identity, banks and credit institutions, fake lotteries and prizes, illegal drugs and services, newsgroup users, pornography, sale of stolen or illegal goods easy at online auction sites, though maintaining anonymity is increasingly difficult.

Source: Compiled from “Superhighway Robbery” (Newman and Clarke, 2003, p.69).

Based on the information in Table 1, three types of information are identified for analysis (See Table 2).

Table 2: Three types of information

Category	Contents	Analysis in dissertation
Personal Identification Information	Name, DOB, Address, SSN, DMV information	Yes
Proprietary Information	- Credit card information - Customer's information - Business transactions - Trade secrets - Medical information - Classified government documents	Yes
Intellectual Property Information	- Patent related documents - Illegal trade of music & movie files - Illegal trade of protected software	Excluded

Source: Compiled from "Superhighway Robbery" (Newman and Clarke, 2003, p.69).

Personal identification includes a person's name, date of birth, address, social security number, and driver's license information. Proprietary information can be credit card information, credit evaluation, customer information, business transactions, trade secrets, medical information, or even classified government documents. Intellectual property pertains to patented documents, music and films, software, and any other original or copyrighted work. For the purposes of this research only the first two categories of information theft will be discussed, while theft of intellectual property will be excluded because it does not pertain to offenses committed by hackers or persons within an organization.

Table 3: Definitions of information theft and data breach

Type	Method	Definition
Information Theft	**Hacking**	- Unauthorized access by outside unknown person. - System compromised by malware/virus/worm/ email.
	Insider Theft	- Information stolen by inside employee/contractor /vendor. - Unauthorized access by inside employee/ contractor/vendor. - Misuse by inside employee/contractor/vendor.
Data Breach	**Stolen/Lost IT Device/Documents**	- Stolen IT device (PC, Laptop, USB or other mobile IT device) by outside unknown person. - IT device is missing by unknown person/method.
	Web Exposure	- Release of secured information found in organization's website. - Release of secured information found in web search engines.
	Mail Exposure	- Secured personal info. mistakenly exposed or delivered to the public through mail or email
	Dumped/lost Document	- Document with customer information leaked to public.

Source: Compiled from OSF and ITRC databases.

By their very nature, government agencies collect and store the private information of citizens (See Table 4), and hold information that could be exploited by enemies of the state.

Table 4: Data Maintained by the U.S. Governments.

Government Level	Data Types
Federal Governments	- Census data. - Corporate tax data. - National security intercepts. - Prison records. - Health records. - Federal employee records. - Contracting and purchasing. - Immigration records. - Personal tax data. - Military records. - Law enforcement data. - Passport applications. - Federal transfer program records (social security, food stamp, and veterans). - Regulatory disclosures, and sealed court records.
State/Local Governments	- State tax data. - K-12 and university educational records. - State transfer programs records. - State prison records. - State contracting and purchasing, - Records deposited in connection with driver's license applications, subject to the REAL ID act. - State law enforcement data. - Records relating to foster children and reported to child welfare agencies. - State court records. - General state data and personal, occupational, and corporate license data.

Source: Froomkin (2009, p. 1023-4).

Before continuing, it is necessary to review official and expert definitions of identity theft, to establish a framework for understanding, research, and discussion. Though identity theft can occur offline, it was a much smaller problem before the spread of the internet, which may account for the fact that the Identity Theft and Assumption Deterrence Act (ITADA), the law recognizing and defining Information Theft, was not passed until 1998. This law defines identity theft as any act in which an individual " knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." The U.S. Government Accountability Office (GAO) defines the term "data breach" as follows: "generally refers to an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers or financial information such as credit card numbers (2007, p.2)." The GAO also notes that "data breaches can take many forms and do not necessarily lead to identity theft." The term "identity theft" is "broad and encompasses many types of criminal activities, including fraud on existing accounts or fraudulent creation of new accounts (GAO, 2007, p.2)." The Federal Trade Commission (FTC) defines identity theft as that which "occurs when someone uses personally identifying information without permission to commit fraud or other crimes (http://www.consumer.ftc.gov/features/feature-0014-identity-theft)." Denning (1999) defines identity theft as the "misuse of another person's identity, such as name, social security number, driver's license, credit card numbers, and bank account numbers (p.241)."

This research focuses on two types of data and information theft: "personal identity information theft" and "data breach." Some information thieves may only pursue personal information, other offenders may seek proprietary information for simple monetary gain. Whether hack or internal breach, information theft is committed for a variety of motives. Those motives determine what kind of information will be stolen, and often how it will be stolen. The most direct example of the relationship between an information thief's goals and the method of their crime is illustrated by the differences of hacking and insider theft. When a hacker attacks a database, success may mean access to the entirety of that database in a mere minutes. As described, personal information can be reproduced with stolen data. For convenience, this dissertation considers the term ‘information theft’ to include the theft of data, as well as the reproduction of information from stolen data.

Chapter Summary

This chapter introduces the problems and issues of information theft, outlines the following chapters, and defines data and information. It also introduces the role of data and information in daily life. Currently estimated volumes of produced data, future prospects of data, and the expansion of information are also introduced. Crimes related to information are presented. The three types of information are outlined: personal identity, proprietary information, and intellectual property.

This chapter explains the terms ‘identity theft’ and ‘data breach.’ The six subcategories of information theft and data breach are outlined: hacking, insider theft, stolen/lost IT devices, information exposure on the Internet, exposure during mail delivery, and dumped/lost documents. This chapter introduces the types of information collected and maintained by governmental organizations. The definitions of identity theft according to the ITAD Act, GAO, and FTC are introduced. The differences between identity theft and data breach are also presented. From stolen data and information, new information can be used for follow up crimes or otherwise exploited by criminal offenders. This research focuses on thefts of data and information. By combining the definitions of identity theft and data breach, the term ‘information theft’ is adopted for this dissertation.

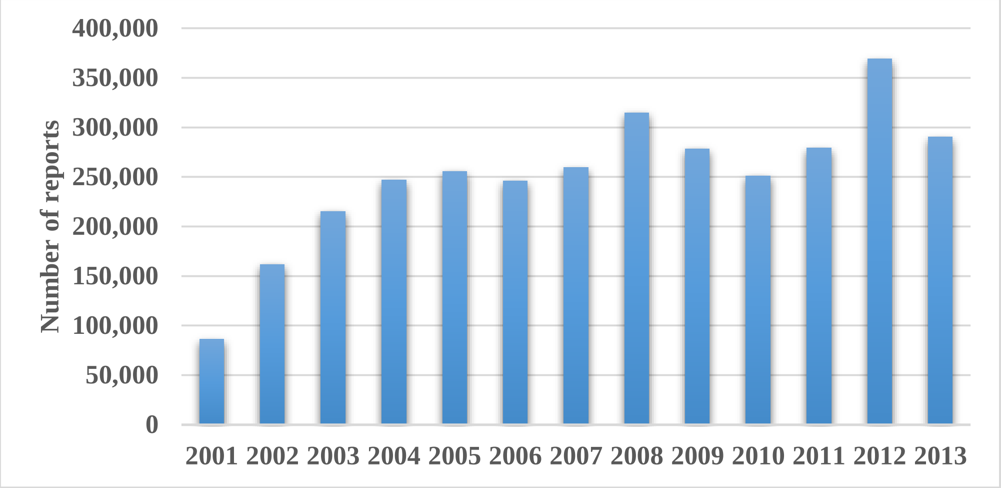
CHAPTER 2: Information Thefts by Offenders and Organization Types

2.1. Overview of Information Theft

Public and private organizations alike hold a range of data to meet their needs. Data may be stolen, exposed, or lost for a multitude of reasons, both malicious and accidental. According to the GAO, data breaches can occur “across a wide range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities” (GAO, 2007, p.5). The term “data breach” is commonly used to describe a situation where data has been stolen, exposed or lost from an organization. Major data breaches are considered to be instances of hacking, IT device theft, stolen documents, insider theft, internet data exposure, data exposure by email delivery error, document or IT device dumping, and the loss of documents (ITRC and OSF). Not all of the aforementioned breaches are cases of identity theft. Hacking and insider theft are likely to lead to identity theft or fraud, but generally are not considered the same offense. At the time of this dissertation there is no research on what forms of data breach lead to direct identity theft and fraud.

The Federal Trade Commission (FTC), the agency responsible for receiving complaints of identity theft, reports that annual instances of identity theft have risen from 86,250 in 2001 to 279,151 in 2011 (See Figure 1). Research indicates that during the World Economy Slump of 2008, cases of identity theft and data breach were filed more than any previous year.

Figure 1: Identity Theft Complaints to the FTC



Source: FTC (http://www.ftc.gov).

According to the National Crime Victimization Survey (NCVS), the percentage of households victimized by identity theft rose from 5.5% in 2005 to 6.6% in 2007 (BJS, 2010). The 2008 NCVS showed an increase in identity theft targeting organizations as well, with 29% of thefts being of personal information during a transaction, 14% of maintained files, and 4% as information leaks over the internet.

Reports by the FTC indicate that the most common form of identity theft between 2002 and 2007 was the creation of fraudulent credit card accounts (See Table 5). From 2008 to 2013, the most common form of identity theft was tax and wage fraud (See Table 5). This fraud has increased dramatically during 2011 to 2013. Identity thefts for government benefits and openings of new utilities have increased. Bureau of Justice Statistics (BJS) reports indicate existing credit card fraud is the most common type of identity theft committed, representing over half of the crimes in that category (Copes 2010, p.1050).

Table 5: Identity Theft Cases Reported to FTC (by percent)

	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	Change
Tax or Wage Fraud	1.9	3.7	3.8	4.8	6.3	8	12.2	12.7	15.5	24.1	43.4	34.7	+
Government Benefits	0.8	1.3	1.4	1.5	1.3	1.4	1.3	1.7	1.8	1.5	1.6	3.9	+
New Utilities	3	3.8	4.2	5.2	5.8	5.2	5.5	8.2	9.4	8.8	6.2	10.1	+
New Accounts Credit Card	24.4	19.2	16.5	15.6	15.2	14.2	12.3	10.2	9.1	8.5	8.8	11.2	-
Driver's License	3	2.3	2.2	1.8	1.5	0.9	0.9	0.9	0.9	0.8	0.6	0.6	-
Business/Personal Loan	2.7	2.3	2.6	2.6	2.5	2.3	1.8	1.8	1.7	1.4	1.3	2.4	
Existing Account Credit card	12.2	12	11.9	11.4	10.7	9.4	8	7	6.7	5.8	4.6	6.1	-
New Wireless	10.6	10.4	10	9	7.2	6.5	4.1	4.6	3.7	3.1	2.5	3.2	-
Employment Fraud	9	11.1	13	12	14	14	15	13	11	8.4	5.4	3.4	-
Electronic Fund Transfer	3.1	4.8	6.6	8	8	7	4.6	4.4	4.8	3.8	3	4.8	
New Accounts Bank	3.7	3.8	3.6	3.3	3.1	3.1	3	3.1	3.2	2.6	1.9	2.2	-
Existing Accounts Bank	8.1	8.2	8.5	7.5	5.8	4	3.4	3.1	2.8	2.3	1.5	1.8	-
Medical	1.7	1.8	1.8	1.9	2	1.6	1.3	1.3	1.3	1	0.7	1.3	-
Attempted ID theft	8	8	6	6	6	5	6	6	7	6.8	6.6	8.4	

Source: Consumer Sentinel Network Identity Theft Complaints (FTC).

Several studies examined the financial impact to companies that disclose privacy or security breaches. Such disclosures to the public have significantly negative impacts on the market value of software sold by respective companies (Telang & Wattal, 2005). A reduction of about 0.6% in stock market prices for a particular company is typical when they disclose a breach (Acquisti, 2006). Because data breaches significantly harm customer confidence, they often go unreported where business is concerned.

2.1.1. Outsider Hacking

In early cybercrime studies, hacking was described as having “evolved into unauthorized access to computer networks (Jordan and Taylor, 1998).” (What is it evolving from, according to Jordan and Taylor?) Contemporary cyber criminals “have evolved their practices to make their crimes more profitable and choose specialties, master their skills, create networks of colleagues, and organize their crimes” (Finklea and Theohary, 2013, p.1). A 2010 study found that “Hackers with a stronger preference for rational decision-making processes seem to engage in preparation, reconnaissance, and attack routines that yield higher success rates than the methods employed by others with a less pronounced preference for rational deliberations.” (Bachmann, 2010, p. 652). The same study found that “[Hackers] are more psychologically rational than intuitive, have high confidence in their technique to problem solving, prefer complex to simple problems, and engage in more risky behavior than the general public.” (Bachmann, 2010, p.652). In accordance with the cautious, reasoned methods of problem solving typical to hackers, it is little wonder that they prefer to steal personally identifiable information (PII) electronically rather than physically (Finklea and Theohary, 2013, p.4). Physical distance offers no protection against hacking when “attacks can be carried out automatically, at high speed, and by attacking a vast number of victims at the same time (GAO, 2009, p.7).” Before attempting a hack, criminals usually take considerable time scanning for vulnerabilities in a network system. Due to daily development of security system (i.e., firewall) by IT security vendors, hackers also need to update their hacking skills and research new trends of Information, Communications and Technology (ICT).

2.1.2. Insider Theft

The U.S. Computer Emergency Readiness Team (US-CERT) defines “insiders” as the following: “A malicious insider is a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems (http://www.cert.org).”

Research by Carnegie Mellon University broke insider crime into the following categories: “1) IT sabotage: an insider’s use of IT to direct specific harm at an organization or an individual, 2) insider fraud: an insider’s use of IT for the unauthorized modification, addition, or deletion of an organization’s data for personal gain, or theft of information that leads to fraud, 3) theft of intellectual property: an insider’s use of IT to steal intellectual property from the organization” (Hanley, 2011, p.2). The research also acknowledged that it is difficult to collect complete information regarding insider threat cases (Hanley 2011, p.4). The full scope of insider theft is immeasurable as a result of being underreported. Of reported insider thefts, 95% occur during normal working hours, over 75% are committed with authorized access, one third continue for over a year, and perpetrators are typically employees with “lower-level” non-technical positions (Capelli 2009, p.18). On average, offenders are employees who have been with their company for over five years, and their crimes go undetected for an average of 32 months (Cummings et al. 2012). Though conducted by different groups at different times, these investigations reveal similar trends in insider theft.

2.2. Information Thefts by Organization Types

To identify organizational types, this dissertation reviewed the industry classification standard maintained by "North American Industry Classification System (NAICS) (see the Table 6)." This classification is used by "federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy."

Table 6: Structure of North American Industry Classification System

Sector	Industry Description	Sector	Industry Description
11	Agriculture, Forestry, Fishing & Hunting	**53**	Real Estate & Rental & Leasing
21	Mining, Quarrying, & Oil & Gas Extraction	**54**	Professional, Scientific & Technical Services
22	Utilities	**55**	Management of companies & Enterprises
23	Construction	**56**	Administrative & Support & Waste Management
31-33	Manufacturing	**61**	Educational Services
42	Wholesale Trade	**62**	Health care & Social Assistance
44-45	Retail Trade	**71**	Arts, Entertainment & Recreation
48-49	Transportation & Warehousing	**72**	Accommodation & Food services
51	Information	**81**	Other services (except Public Administration)
52	Finance & Insurance	**92**	Public Administration

Source: U.S. Census Bureau (http://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012).

2.2.1. Information Thefts in Business

Hacking incidents at business organizations.
(The Washington Post. March 24, 2014. "U.S. notified 3,000 companies in 2013 about cyberattacks)
Source: http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html

> *“Federal agents notified more than 3,000 U.S. companies last year that their computer systems had been hacked, White House officials have told industry executives, marking the first time the government has revealed how often it tipped off the private sector to cyber intrusions.*
>
> *The alerts went to firms large and small, from local banks to major defense contractors to national retailers such as Target, which suffered a breach last fall that led to the theft of tens of millions of Americans’ credit card and personal data, according to government and industry officials.*
>
> *“Three thousand companies is astounding,” said James A. Lewis, a senior fellow and cyber policy expert at the Center for Strategic and International Studies. “The problem is as big or bigger than we thought.”*
>
> *The number reflects only a fraction of the true scale of cyber intrusions into the private sector by criminal groups and foreign governments and their proxies, particularly in China and Eastern Europe. The estimated cost to U.S. companies and consumers is up to $100 billion annually, analysts say.”*

An examination of 274 cases of identity theft prosecuted by the Secret Service from the year 2000 through 2006 found that about 50% resulted from a compromise in data at a business (Gordon, 2007). Internal, illegal misuses of data often go undiscovered in the business sector (Cappelli et al. 2006). Symantec disclosed in a survey that two thirds of business organizations had lost information in the previous twelve months, “due to causes such as human error, hardware failure, software failure and lost or stolen mobile devices.” (Symantec, 2012, p.9). Information theft has a devastating impact where business is concerned. Reports indicate the impacts of a data breach are as follows “lost customers (49%), damage to the brand (47%), decreased revenue (41%), increased expenses (39%) and a tumbling stock price (20%)” (Symantec, 2012, p.9). Following a data breach, business is disrupted by 61%, 58% of sensitive information is lost, 25% of finances are lost, and reputation is damaged by 13% (Ponemon, 2012, p.17). The same study claiming

61% business disruption finds that the primary goal of cyberattacks against a business are financial fraud and access to financial records. A successful breach of a business's network will yield about 70% of their financial records, 55% of their customer data, 53% of their intellectual property, and 12% of their employee records. From this information it is clear that, as one would expect, the majority of cyber infiltrations targeting businesses are perpetrated for monetary gain.

2.2.2. Information Theft in Education

Though less prevalent than in other fields, information theft at higher educational institutions is not commonly heard of. However, the below New York Times report presents an exact description of information theft incidents at American universities.

Hacking incidents at higher educational organizations.

(The New York Times. July 16, 2013. "Universities Face a Rising Barrage of Cyber attcks")
Source: http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all&_r=0

"America's research universities, among the most open and robust centers of information exchange in the world, are increasingly coming under cyberattack (....)."

"(....) They acknowledge that they often do not learn of break-ins until much later, if ever, and that even after discovering the breaches they may not be able to tell what was taken (....)."

" (....) Universities and their professors are awarded thousands of patents each year, some with vast potential value, in fields as disparate as prescription drugs, computer chips, fuel cells, aircraft and medical devices (....)."

"(.....) A university environment is very different from a corporation or a government agency, because of the kind of openness and free flow of information you're trying to promote," said David J. Shaw, the chief information security officer at Purdue University. The researchers want to collaborate with others, inside and outside the university, and to share their discoveries (....)."

Of 72 surveyed colleges and universities, 11 had suffered information theft at least once (15%), more than two-thirds lost data from stolen laptops, 54% experienced copyright violations such as pirating from the school network, 50% suffered a denial of service attack, 37% had areas of restricted access breached, 22% had their websites defaced through hacking, 21% experienced accidental information leaks through email, 7% encountered fraud, and 4% experienced a violation of intellectual property (Burd, 2008).

A 2011 report by Security Application, Inc. (presently renamed Trustwave) indicates “budgetary constraints represent the most reason for a high volume of attacks in higher educational institutions. This is evidenced by a new report stating that only 50% of universities in the U.S. plan on increasing their IT security spending for 2010” (p.3). Further, according to the Enterprise Strategy Group (2011), IT security financing was highest in financial service sectors. The lowest increase in IT spending was for educational institutions (Security Application, Inc., 2011).

2.2.3. Information Theft in Healthcare

Hacking incidents at medical organizations.

(Los Angeles Times. August 18, 2014. “Hackers stole 4.5 million patients' data in hospital
breach”)
Source: http://www.latimes.com/business/technology/la-fi-tn-community-health-hacked-20140818-story.html

“Cyberattack……stole Social Security numbers and other personal data for 4.5 million patients whose records were in Community Health Services Inc.’s system, the company said Monday.

The data breach included the names, addresses, birth dates, telephone numbers and

> *Social Security numbers of patients who were referred for or received services from doctors affiliated with the hospital group in the last five years. It did not include patient credit card, medical or clinical information, the company said in regulatory filings.*
>
> *Tennessee-based Community Health is one of the largest hospital groups in the U.S., operating 206 hospitals in 29 states. It has three hospitals in California: Barstow Community Hospital, Fallbrook Hospital and Watsonville Community Hospital (....).”*

The Electronic Health Records service (EHR) and healthcare portals for patients and providers have made it easier to access and share medical information. While ease of access is necessary for improving patient care and safety, it unfortunately makes it easier for criminals to gain access to information which can be exploited. Where medical facilities are concerned, there are information thefts of individual data as well as organization data. The 3rd annual survey of the Ponemon (2012, p.7) interviewed victims to study the causes of medical identity theft: 22% of respondents’ identities were used by their healthcare providers to conduct fraudulent billing, and 7% of respondents’ identities were stolen by employees of their healthcare office. Medical identity theft victims are usually older, 61% being over 36 years old. Identity Force (2009, p. 4) disclosed in its national survey of hospitals that 63.3% of hospitals reported at least one data breach annually, while 20% reported ten or more a year. These results imply that data breaches may be under-reported. The “ID Experts” (2009, p.4) noted that 52% of large hospitals (more than 300 beds) experienced a data breach in the past year compared to 33% of medium-sized hospitals (between 100 and 300 beds) and 25% of small hospitals (less than 100 beds). It may be that data breaches in large hospitals are more likely to be reported to the public due to the ARRA and HITECH acts, or that smaller hospitals actually experience fewer data breaches.

2.2.4. Information Theft in Government

Hacking incidents at governmental organizations.

*(CNN. December 17, 2014. “*Government hacks and security breaches skyrocket*”)*

Source: http://www.cnn.com/2014/12/19/politics/government-hacks-and-security-breaches-skyrocket/

“(….) A CNN review of cyber attacks against federal agencies shows at the number of breaches into government systems is skyrocketing.

"Espionage is happening at a rate we have never seen before," said Denise Zheng, a deputy director at the Center for Strategic and International Studies.

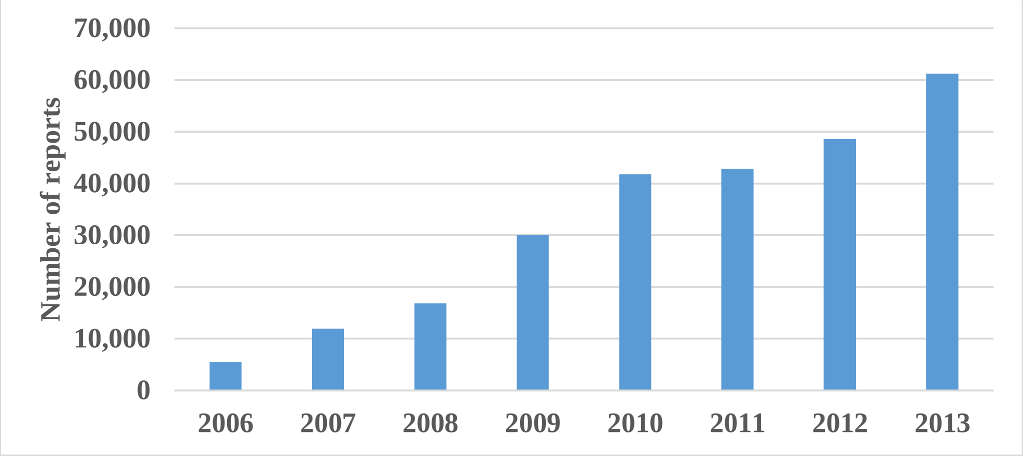
The numbers seem to bear that out. There were almost 61,000 cyber attacks and security breaches across the entire federal government last year according to a recent Obama administration report.

And the number of cyber incidents involving government agencies has jumped 35 percent between 2010 and 2013, from roughly 34,000 to about 46,000, according to another recent report by the Government Accountability Office (….).

(…) Unclassified networks at the White House and State Department were recently hacked, leading the State Department to shut down its email system for days last month (…).”

Government agencies are a preferred target for information thieves. As a target, the government may have a symbolic attraction for hackers, who hope to increase their reputation by successfully breaching a federal network. The number of IT security incidents reported by federal agencies to US-CERT has increased from 5,503 incidents in the fiscal year 2006 to 61,214 incidents in the fiscal year 2013 (Figure 2).

Figure 2: Incident reported to US-CERT by 24 federal agencies in 2006-2013



Source: GAO analysis report of US- 3CERT data (2014).

The four most prevalent types of incidents reported to US-CERT by the federal government during the fiscal year 2011 were malicious code (11,626 instances), improper usage (8,416 instances), unauthorized access (6,985 instances), and scan, probe and attempted access (2,942 instances) (GAO, 2012, p.9). GAO (2012) indicates that given the above vulnerabilities and assessments, negative impacts of cyber attacks on government systems include:

> “loss or theft of resources, such as federal payments and collections, inappropriate access to and disclosure, modification, or destruction of sensitive information, disruption of critical operations supporting critical infrastructure, national defense, or emergency services, undermining of agency missions due to incidents that lose the public’s confidence, and use of systems for unauthorized purposes or to launch attacks on other computers systems (p.2).”

As national infrastructures have become dependent on data systems and networks, the interconnectivity between data systems, the internet, and infrastructures may provide opportunities for criminals to disrupt critical IT systems (GAO, 2011b, p.2.).

2.3. Laws Related to Information Theft

The Computer Fraud and Abuse Act, enacted in 2001, “defines computer crime offenses including intentionally accessing a computer without authorization or exceeding authorized access to obtain financial and credit card information” (Gerard et al., 2004, p. 36). The Fair Credit Reporting Act was altered by new amendments under the Fair and Accurate Credit Transactions Act, enacted in 2003, with sections designed to combat identity theft (Stevens, 2010). The Gramm-Leach-Bliley Act, enacted in 1999, directs financial institutions to have “policies, procedures, and controls to prevent the unauthorized disclosure of customer financial information and to deter fraudulent access to such information” (Newman & McNally, 2005, p. 67).

In medical sector, the Health Insurance Portability and Accountability Act was enacted for protection from identity theft in 1996. It outlines “legal penalties for individuals or agencies when use personal health identifiers or cause them to be used or that provide individually identifiable health information (Gerard et al., 2004).**”** In 2009, the Congress strengthened the HIPAA privacy and security requirements and added a federal framework for data breach notification (American Hospital Association, 2010).

In the federal sector, the Privacy Act of 1974 is the principal law governing the federal government’s information privacy program. Other relevant federal laws are the Computer Matching and Privacy Protection Act of 1988, and the E-Government Act of 2002 which “requires federal agencies to conduct privacy impact assessments on new information technology systems and electronic information collections.” Federal Information Security Management Act (FISMA) is the principal law governing the federal government’s information security program. This act requires federal government agencies to provide information security protections (Stevenson, 2010). The Office of Management and Budget (OMB) requires all federal agencies to implement a breach notification policy to safeguard “personally identifiable information.”

According to National Conference of State Legislatures (2015), forty-seven states except Alabama, New Mexico, and South Dakota, have passed “Security Breach Notification laws to require businesses and/or government agencies to notify persons affected by data breaches and to implement information security programs to protect the security, confidentiality, and integrity of data. These laws also requires organizations to implement a breach notification policy, and include requirements for incident reporting and handling and external breach notification. Typically these Data Breach Notification law requires organizations to notify any data breach affecting more than 500 residents of a State to affected victims. Specifically, the aforementioned HIPPA Breach Notification Rule, 45 CFR, required entities to “provide its breach notice to prominent media outlets serving the State or jurisdiction (HHS, 2014).”

2.4. Research Issues in Information Theft

Roberds and Schreft (2009, p.4) assert that there is no definitive estimate of how many cases of identity theft have resulted from data breaches, but breaches are numerous, and rising. They further note that a data breach will not necessarily result in identity theft, as data may be stolen without being used for fraudulent purposes, though they may appear to be the same as identity theft**.** Recorded incidents of PII being lost or stolen may not all be actual cases of identity theft. Other information can be obtained from “public records or other data thefts and combined to obtain more complete identification records, increasing the odds that the owners of the information become victims of identity theft" (Schreft, 2007, p.7). Schreft also points out that compromised records are misrepresented because in many cases the number of records lost or stolen is unknown or not disclosed (p.8).

According to the 2010 CSI Computer Crime and Security Survey, 27.5% of businesses that experienced breaches of IT security reported intrusions to law enforcement, 25.4% of victim organizations did not disclose intrusions to the outside, and 18.1% of organizations informed targeted customers of intrusions (p.24). Only 3.6% of organizations released news of an intrusion to public media. The survey also provides some reasons why affected organizations are not willing to report damage caused by information theft. First, many organizations believe law enforcement is incapable of correcting such damage. Second, some incidents are too small to report. Third, there is a concern that news of a breach in information security may hurt stock value and brand image. Fourth, competitors may capitalize on a business that has been weakened by a hack or insider theft.

Among hospitals and clinics there is also a reluctance to report identity theft to law enforcement. About half of medical identity theft victims do not report the crime to law enforcement agency because they know the thief personally. 45% of medical identity theft victims did not think the police could help. 39% were caused no detriment by the theft, and 9% did not have time to file a police report (Ponemon report, 2012, p.6). This is one area where greater news coverage could contribute to a more accurate log of data breaches, which would support analysis in information theft research.

Unfortunately, measuring the extent of a data breach or identity theft has many limitations. Unlike crimes of violence or crimes against physical property, information theft victims can be completely unaware that they have been attacked, and often times they are. Damage is not readily visible, and can be more serious than victims realize. At the time of this dissertation there are no publicly recognized law enforcement agencies specific to information theft cases, and law enforcement maintains no official records of information theft incidents. Combined with many victims of information theft being unwilling to deal with the police, information useful for the research of information theft and data breaches is extremely limited.

Currently, there is a surge of smart phone and tablet theft which may not be reflected in present data breach statistics. Business and medical professional are increasingly storing and accessing “sensitive” data in these mobile devices. News organizations recently reported a sudden increase of smart phone robbery in urban areas. Whether or not larcenists of smart phones are interested in the data they store, it is obvious that the frequency of stolen or lost IT mobile devices is dramatically increasing.

Surveys on cybercrime and data breach which are helpful to this kind of research are typically met with an underwhelming number of participants. For example, in the 2010 CSI Computer Crime and Security Survey, survey questions were sent to 5,412 security practitioners, and only 351 were answered: a 6.4% response rate. Ponemon surveys also receive few responses; in data breach studies they received responses from 3.4 and 4.5% for two years (See table 6). It is difficult to accurately measure information security with so few results; unwillingness to participate in data breach surveys may be a result of fear of damaging company image and customer confidence, however.

In several data breach studies conducted by Ponemon, The Computer Security Institute, and Carnegie Mellon University, the majority of respondents (76.8%) were businesses; 10.9% of respondents were government agencies, 7.9% were healthcare offices, and 5.5% were colleges and universities. Based on this sample, schools and hospitals/clinics are drastically underrepresented in data breach statistics. Cases collected for this dissertation are composed 58% from businesses, 14.1% from educational institutions, 19% from places of medical treatment, and 10.9% from government. Because it is required by law, data breach cases in medical organizations are reported to the public more frequently than in other organizations.

Table 7: Comparison of data breach studies

	Sample Size	**Year**	**Response Rate (%)**	**Response Organizations' Distributions**			
				Business (%)	**Education (%)**	**Medical (%)**	**Government (%)**
Ponemon survey 1	725	2012	4.5	73	2	11	15
Ponemon survey 2	843	2011	3.4	79	4	8	9
CSI survey	351	2010	6.4	77.1	8.9	6.6	7.4
Carnegie Mellon Univ. survey	523	2010	n/a	78	7	6	9
Average proportion (%)				76.8	5.5	7.9	10.1
Dissertation samples (N=1,003)				58	14.1	19	10.9

Chapter Summary

Chapter Two summarizes the general scope of information theft, introducing the two scopes: insider theft and outsider hacking; the methods of information theft: information theft in business, education, healthcare, and government; laws related to handling identity theft and data breach, and research issues in the study of information theft. Many organizations maintain sensitive data and information vulnerable to exploitation. Annual identity theft and data breach incidents have increased according to NCVS, FTC, and ICCC/FBI statistics. The impacts of information theft on affected organizations can be tremendous.

This research analyzes two types of information theft: hacking and insider theft. Insider theft is difficult to discover due to the fact that insiders are extremely knowledgeable about their organization's IT management system. Outside hackers tend to spend a certain amount of preparing to attack their target IT system. Hackers' activities are different from traditional criminals'. Successful hackers will have advanced IT skills.

Several research studies show that the majority of businesses experience information theft. There are very few studies regarding information theft in educational organizations. However, a majority colleges and universities have experienced various types of IT security incidents. A majority of medical organizations are vulnerable to data breach, and these breaches are under-reported. Government organizations are popular targets for hackers, as either a symbolic target or an opportunity to raise reputations. U.S. CERT shows a steady increase of IT security incidents among federal agencies.

The Gramm-Leach-Bliley Act, Computer Fraud and Abuse Act, Health Insurance Portability and Accountability Act, Privacy Act of 1974, Computer Matching and Privacy

Protection Act of 1988, the E-Government Act of 2002, and the Federal Information Security Management Act (FISMA) are the major laws related to data breach and privacy protection to date.

Regarding research issues, there are no studies measuring the full scope of information theft. Survey response rates are very low. Some organizations are unaware they’ve suffered an information theft, while others are unwilling to disclose a breach.

CHAPTER 3: Theoretical Framework

3.1. Rational Choice Theory

A priority of this research is to explain how information theft occurs, and how criminals go about choosing a target for information theft before committing cybercrimes. Rational Choice theory dictates that criminals commit crimes after weighing the benefits of the crime against the cost of being caught and punished. (Becker, 1968; Cornish and Clarke, 1986, 2000). According to Cornish and Clarke (1986), this theory asserts that those who commit a crime engage in a calculated, utility-maximizing behavior: seeking maximum reward at minimum cost. From this disambiguation, criminals are considered to be rational, determining before a crime whether or not to commit it, and how it will be committed. In summary, the theoretical frameworks of Rational Choice Theory are: the decision to commit a crime may be rational, the decision to commit a crime is often an informed decision, the information needed to commit a crime varies with the type of crime to be committed, and the decision to commit a crime will be affected by the immediate contextual characteristics of the crime (Cornish and Clarke, 1987). In essence, crimes are committed, or not committed, based on situational factors. Cornish and Clarke (1987) conceptualized this decision making process as the 'choice structuring properties' of different crimes. Choice structuring properties include reviewing properties such as rewards, risks, personal enjoyment, and possible obstructions.

Criminals rarely have complete information on the environments or situations of targets. The decision-making process is limited to certain ‘environmental’ or ‘situational’ factors, such as time, the cognitive capacity of the criminal, and available information, resulting in a ‘limited’ or ‘bounded’ rationality rather than a complete rationality

(Cornish & Clarke 2008). The “limited” or “bounded” nature of rationality comes from the time and effort a crime requires, combined with the relevant information available to the person preparing to commit the crime (Felson and Clarke, 1998). Like other criminals, hackers’ decision-making process is based on “bounded rationality.” They are rarely capable of knowing the full extent of IT security measures protecting their target organizations. Skill is often not sufficient by itself for obtaining information from target organizations. Therefore, hackers search for vulnerabilities in IT security systems before initiating a cyberattack. Even when successful in obtaining desired information, hackers still have a risk of detection by IT security, and eventual arrest. Inside offenders, however, have enough knowledge of the information security at their organizations to determine how and when to steal the desired information without being detected. Because, as outlined by Rational Choice Theory, decision making varies by crime type, hackers in pursuit of financial information are more likely to attack a bank than, say, a college. Insider theft differs in that rather than attempting to gain unauthorized access to a computer, an insider might steal the entire computer. To prevent a crime of information theft, the opportunity structure of each individual crime must be analyzed. Rational Choice Theory is well suited to investigating the decision-making processes of information theft, when compared to other theories in criminology.

Hackers often seek targets beyond their own national borders. Consequently, tracing the origins of a hack requires professional employees and specialized equipment. Hackers’ skills often exceed those of the IT security staff at organizations they attack. Due to limited budgets, organizations become vulnerable to attack by not allocating enough money to the upkeep and upgrade of their IT security systems. Hackers are well aware of this weakness. Inside offenders are exceedingly aware of the weakness, and sometimes they are members of IT security themselves.

3. 2. Situational Crime Prevention Theory

Situational crime prevention theory (SCPT) emphasizes the ‘situational determinants’ of crime and offers a range of techniques and strategies for crime prevention and reduction. SCPT pays specific attention to the role of opportunity in anticipating and preventing crime. To understand why crimes happen, attention must be shifted from criminal dispositions or motivations, to the opportunity structures allowing crimes to occur (Clarke, 1980). According to SCPT, opportunities for crime are not randomly distributed, but rather are concentrated in certain times and spaces. Certain locations are more prone to crime than others, and certain crimes occur during specific time periods. The SCPT suggests that law enforcement should focus on “opportunity reduction” by devising strategies that reduce criminal opportunities (Cornish and Clarke, 2003). The SCPT offers the following strategies to deter criminal activity: increasing the risk factor of attempting to commit a crime, increasing the effort needed to commit a crime, reducing the rewards of a crime, reducing provocations, and removing the excuses for committing a crime (Cornish and Clarke, 1986). These strategies apply particularly well to information theft prevention. Hacking from outsider and insider theft may be reduced with more frequent, strengthened security measures of organizations’ information management systems. From the viewpoint of the SCPT, the immediate assessment of those systems should take precedent over any service to customers who could become the victims of information theft committed via a breach in those systems.

From the premise of the Rational Choice Theory, it is anticipated that the target selection process of information theft, from outside or inside, would not be random, but rather dependent on the low level of risk in being detected and high level of reward (value of available information). Rational Choice Theory and Situational Crime Prevention Theory may facilitate understanding why some organizations are more vulnerable to information theft than others. Even when an organization has tightly-managed IT security, there will inevitably be loopholes inside and outside of the system. Finding those loopholes is merely a matter of time for determined hackers. Depending on their preferences, hackers may look for financial gains from small organizations with vulnerable systems, or they may look for an increased reputation through cracking a more elaborate system. Hackers' decisions are guided not only by the availability of sought after information, but by the likelihood of detection as well. Newman and Clarke (2003) proposed a practical model of "Opportunity-reducing techniques in the e-commerce environment", expanded from Clarke's outline of 'The Four Main Ways of Reducing the Opportunities for Crime' model (1997.). Newman and Clarke's model is a detailed, comprehensive guide for preventing crime in the e-commerce sector. The model this research proposes for preventing information theft is based on that model.

3.3. "SCAREM" Analysis

Clarke (1999) developed the acronym "CRAVED" to explain the elements that make certain consumer products more vulnerable to theft than others. He designated these products "Hot Products", and explained the basis of their vulnerability with the acronym "CRAVED." The attributes of CRAVED are Concealable, Removable, Available, Valuable, Enjoyable, and Disposal. Newman and Clarke (2003) revised the initial attributes of “CRAVED” to form the “SCAREM” model of e-commerce related crime. As stated earlier, this dissertation adopts the “SCAREM” model for analyzing the characteristics of information theft. The “SACREM” model “identifies the elements of the information system itself that are conducive to crime with the acronym SCAREM: Stealth, Challenge, Anonymity, Reconnaissance, Escape, and Multiplicity” (p.61). Further, “Those six features, SCAREM, identify not only features of the information system that are 'hot' in and of themselves, but also tie these to the known motivations of potential offenders” (p.61).

SCAREM Information

Stealth

“Stealth” describes the virtual invisibility the internet offers. This feature is “certainly a ‘convenience’ provided to all who use the internet.” This is one of the main difficulties in tracing hackers across cyberspace, made more of a problem by advanced hacking skills, vulnerabilities in IT security systems, a lack of IT professionals in law enforcement, the tendency of hackers to seek targets outside their borders, and a reliance on digital evidence.

Challenge

“Challenge” is often times part of the appeal for a hacker attempting to steal information. One motivation is “to beat the computing system” (Newman and Clarke, 2003, p. 61). As stated earlier, hacking requires a great deal of energy and preparation, which in turn demands some degree of obsession. With a certain level of preparation, “to carry out the intrusion virtually under the noses of the computer administrator (p.62),” "the risk of getting caught can be reduced to zero" (p.62). Compared to the preparation process, the act of information theft itself takes very little time.

Anonymity

"Anonymity" is abundant on the internet. Crossing over somewhat with stealth, this factor makes it difficult to track the location and identity of hackers, thanks to there being a multitude of ways to avoid IP address tracking. Further, it allows "hackers to spend long periods of time online attempting to gain illegal entry into [a target IT system]" (Clarke and Newman, 2003, p.62). Wortley noted that the power of anonymity breeds irresponsible or criminal behavior (Clarke and Newman, 2003).

Reconnaissance

For the criminal, according to Rational Choice Theory, choosing a vulnerable target is of paramount importance. "Reconnaissance" describes the process hackers take to look for "holes" or "gaps" in an IT security system before they carry out their attack. An informed criminal tends to make careful reconnaissance of all possible targets, then act accordingly (Clarke and Newman, 2003, p.63). Hackers generally do not attack a system without first conducting some surveillance.

Escape

Pursuant to the factors of stealth and anonymity, "Escape" comes naturally for hackers, giving them plenty advantage over law enforcement. Cybercrimes are often undetected and, as stated, more often than not victims of information theft are unaware they've been attacked.

Multiplicity

Cybercrime tends to beget more cybercrime, and this is where “Multiplicity” comes in. One cyber offense “can be multiplied exponentially” (Clarke and Newman, 2003, p.63). This means, for example, that bank accounts stolen through a hack can be extorted to the victim. One cybercrime can present the possibility of another.

3.4. Seasonal Variation

There are several studies suggesting seasonal patterns in property crime. Block (1984) found that burglary and larceny/theft have seasonal fluctuations. He found that the theft of unattended property, personal property, and property left outside people’s homes was most common in the summer. BJS reports (1988) indicate personal larceny with contact and unlawful entry are both highly seasonal (p.10). Hird and Ruparel (2007) found that 25 of 29 established types of crime show seasonal patterns. Specifically, they found that non-domestic burglary occurs most frequently in May. Lauritsen and White (2014) also found that household larceny and burglary exhibit seasonal patterns, with the highest frequencies taking place in the summer” (p.4). There are however very few studies of seasonal variations in cyber hacking. Because the internet is easy to access, it is assumed that no particular time of the year is more suited to cyberattacks than another.

Chapter Summary

This chapter provides the theoretical frameworks of Rational Choice Theory for explaining the characteristics of information theft. The perspective of Situational Crime Prevention Theory is adopted to develop policy implementations for information theft prevention. Because neither hackers nor inside offenders are impulsive criminals, Rational Choice Theory is applied to them by examining their selection processes. It could be hypothesized that certain types of organizations appeal to hackers and insiders differently depending on certain criteria. This research develops techniques for information theft reduction based on the 25 technique model created by Newman and Clarke (2003). The SCAREM model was developed to explain the characteristics of offenses in e-commerce, and is used in this research to explain the characteristics of information theft in four types of organizations. Reports of information theft are also tested for seasonal variations. Several research studies found that there are seasonal variations in many traditional crimes, this research studies whether or not those same patterns exist in information theft.

CHAPTER 4: Research Design

As stated, the goals of this research are to examine the kinds of organizations that are vulnerable to outsider hacking and insider theft, to determine if organization size is a factor in information theft vulnerability, and to explore whether or not the time it takes to discover an incident of information theft varies with the nature of the theft and the type of organization being attacked. This dissertation also addresses research issues related to pursuing a prevention model. Factors related to risks of outsider and insider thefts at different types of organizations are examined based on the preliminary data analyzed in this research. Due to the limited internal characteristics of the data available, this research does not test variables for the application of Rational Choice Theory. However, to achieve the primary purpose of this research: identifying the environmental factors of information theft; research questions are inferentially guided by the Rational Choice Theory.

4.1. Research Questions

With the assumptions of this dissertation guided by Rational Choice Theory and Situational Crime Prevention Theory, the following three research questions are posed:

Research Questions

RQ 1	**What kinds of organizations are vulnerable to what kinds of information theft?**
RQ 2	**Does the time taken to detect information theft vary with the nature of the theft and type of organization?**
RQ 3	**Does information theft show any seasonal variation in organizations?**

4. 2. Hypotheses

Different organizations have different types, and levels of IT security systems for data and information protection. Those differences are dependent upon the types and characteristics of organizations, the available budgets for security, implementations of security policies, and organizational leadership's attention to data and information protection. Insider thieves collect, process, and manage valuable data and information as part of their daily work routines. Not all insider thieves are highly skilled experts, but they inevitably know how to search, review, and print the data and information they want to steal. They know when routine monitoring and assessment are conducted on their organizations' IT system. While employed, insiders are up to date with the vulnerabilities of the IT system protecting the information they wish to steal. Accordingly, insiders have the advantage of being able to cover their tracks for a period of time, or even erase the evidence of their theft completely. Their offenses may be a one-time event: No one will suspect insider theft until customers notice they've had their identity stolen, or a routine IT system assessment reveals the breach. It is assumed that larger organizations will suffer more information theft because they would have too many employees to properly monitor and would have more valuable information. However, smaller organizations are often more vulnerable to information theft due to limited budgets insufficient for proper information protection. Employees in smaller organizations are more likely to know the structure of their IT security system when compared to employees in larger organizations.

There are several measures available for protecting data and information in any organization, yet the level of IT surveillance varies greatly between them. The budget and staffing of IT security can make a major difference in information theft prevention. As simple a solution as this is, it is frequently overlooked. If an information theft remains undiscovered for an extended period of time, it is assumed that the victim organization does not maintain a well-organized monitoring system. Regarding detection time for the theft of data and information, it tends to take longer to detect insider theft, versus outsider hacking. Exploring the periods of detection time between the time of offenses and the time of detections is the first step in developing countermeasures against data and information theft incidents. By this basis, the guidance of The Rational Choice Theory, and relevant studies of information theft, this research offers the following hypotheses:

Hypotheses

H1	**Hacking incidents are more likely to occur at smaller organizations.**
H2	**Insider theft incidents are more likely to occur at larger organizations.**
H3	**Governmental organizations will likely experience higher rates of information theft.**
H4	**Insider theft incidents will take a longer time to detect.**
H5	**Governmental organizations will detect the information theft more quickly.**
H6	**Information theft incidents are not likely to show seasonal variation.**

4. 3. Unit of Analysis

In this research, the unit of analysis is an incident of information theft (insider theft or outsider hacking) occurring in four types of organizations: business, education, healthcare/medical, and government.

4. 4. Dependent and Independent Variables

4. 4. 1. Dependent Variables: Incident rate of information theft

Incidents of insider theft and hacking studied in this dissertation were catalogued based on the databases of the Open Security Foundation, Identity Theft Resource Center, and Department of Public Health and Human Resources. For the purposes of this research, one instance of insider theft is equivalent to a onetime event of outsider hacking or insider theft taking place in the period of 2007-2013 Each individual case of information theft includes a method, a specific organization being targeted, a time of theft, a detection period (how long the crime went unnoticed), and a brief description of the incident. Unfortunately, not every case of information theft found in the aforementioned databases provides all this information, so each case will not necessarily fill all the above fields.

For use with the following three research questions this dissertation has devised calculations for “information theft rates.” Because each industrial sector has different numbers of firms, when the same amount of incidents occur in, for example, finance and retail sectors, the information theft rates will still differ. Precise calculation of information theft rates is necessary in order to identify the factors protecting data and information in any given organization. The information theft rates were measured as follows:

1) Numerator: total identified incidents per industrial sector.

The numerator of each information theft rate is equivalent to the total identified incidents per industrial sector, as reported by the cited databases from 2007-2013.

2) Denominator: total number of firms per industrial sector.

The denominator of each information theft rate is equivalent to the number of firms belonging to that sector. The numbers of firms as claimed in this research are based on the U.S. Census Bureau’s records. The definition of firm is defined by the U.S. Census as follows:

> “A firm is a business organization or entity consisting of one domestic establishment (location) or more under common ownership or control. All establishments of subsidiary firms are included as part of the owning or controlling firm. For the economic census, the terms "firm" and "company" are synonymous (U.S. Census, 2014).”

Pertinent data collected in this dissertation does not apply to all four types of organizations outlined in this research, and is therefore limited in describing the characteristics of information theft. The collected data in this research does not cover the entire numbers of data incidents in the United States. As mentioned earlier, there is no national level of database for disclosing the data and information incidents. Some State Attorney's Offices are receiving data breach notifications from the affected entities in their states. Citizens may access to these notified incident data by the State Freedom of Information Laws. Information incidents affected more than 500 citizens are required to be released to major local media by the HIPPA law. The two databases used in this dissertation collects the information incidents from the public media and some selected State Attorney's Offices, i.e., N.Y., M.A., and M.D. Those databases are still maintaining comprehensive and useful resources for information theft research even these databases do not cover the entire information incidents in the U.S. Therefore, those information incident rates do not indicate the exact rates of information theft at each industrial sector. However, the estimated information theft rates in this research may be useful to figure out the characteristics of information theft in a limited range.

4.4.2. Independent Variables

The independent variables of this research are organization type (business, educational, medical, and government), organization size (based on number of employees or students in an organization), and the time periods between the occurrence of incidents and their discoveries.

4.4.2.1. Types of Organizations

As previously established, this dissertation considers “organizations” to be any firm of one of the following sectors: business, education, healthcare/medical or government, based on The North American Industrial Classification System (NAICS). This categorization is outlined below Table 8.

Table 8: Organizational Types by the NAICS

Organizational Type	NASICS Code	Industrial sector	Sub-industrial sector
Business	22	Utilities	Energy
	31-33	Manufacturing	Manufacturing
	42	Wholesale Trade	- Wholesale/Retail Trade - Car Dealer - Gas Station
	44-45	Retail Trade	
	48-49	Transportation and Warehousing	Transportation
	51	Information	Publishing/Media/Broadcasting
			Software/IT Service
			Telecommunications
			Data Processing Service
	52	Finance and Insurance	Bank
			Financial Institution
			Insurance
	54	Professional, Scientific, and Technical Services	Professional/Technical Service
			Tax Service
	56	Administrative and Support and Waste Management and Remediation Services	Administrative/Support Service
	72	Accommodation and Food Services	Hotel
			Food Service
Education	61	Educational Services	Higher Educational Organizations
Healthcare/ Medical	62	Health Care and Social Assistance	Hospital
			Medical Clinics
			Healthcare
Governmental	92	Public Administration	Federal Government
			State Government
			City Government
			Local Government

Source: U.S. Census Bureau (http://www.census.gov).

4.4.2.2. Organization Size

The standards of size ranges apply differently to different types of organizations. For example, businesses with 500 or fewer employees are very common, while there are few colleges or universities with 500 or fewer students. Based on these discrepancies, a single size classification is not sufficient to for this research. For businesses, both single and multi-establishment firms were analyzed, including the sub-categories: utilities, manufacturing, wholesale and retail trade, transportation, information, finance and insurance, professional, and technical services, administrative and support services, accommodation, and food services. The size of those business organizations is measured by the number of total employees. Medical organizations are categorized as hospitals (or medical centers), medical clinics and healthcare services. The size of these medical organizations is determined by the amount of staff. Educational organizations include two and four year colleges and universities; their size was determined by the amount of enrolled undergraduate and graduate students, omitting faculty. Governmental organizations divide into the subcategories of federal, state, city and local governments. Federal agencies and departments are naturally assumed to be the most abundantly staffed. Local governments are assumed to be less staffed.

4.4.2.3. Detection Time Period of Incidents

In order to answer RQ 2, this dissertation explores the detection periods of information thefts: the time between the moment information is stolen and the moment the theft is detected. As suggested in several prior sections, data suggests a gap between the detection period of insider thefts and outsider hacks, attributed to varying characteristics between the two crimes as well as variances in IT security systems.

Identifying these differences could prove beneficial for IT threat assessment and general readiness.

The continual evolution of hacking techniques makes detecting a hacking incident increasingly difficult. Detection can take weeks, or months depending on the hacker's skill and the proficiency of the affected organization's IT security team. Often times, hacking incidents are detected quickly only because the person or group responsible for the crime discloses it to the public. Even the most consistently updated IT security system does little in the way of detecting and preventing hacking. As discussed, insider thefts are even more difficult to curb. Some insider thefts may remain undetected for years. Insiders can be detected more quickly by an organization with efficient IT security management, but even that is of limited power.

4.5. Data Sources

At the time of this dissertation, there are some government efforts to track information theft, though there is no complete record of those crimes. Occasionally, the Bureau of Justice conducts the National Crime Victimization Survey and collects reports of information theft, though very few. The Internet Crime Complaint Center of the FBI releases an annual complaints analysis report regarding cybercrimes including identity theft, and those complaints are traditionally forwarded to The Federal Trade Commission. The U.S. Department of Health and Human Services posts a summary of data breaches in hospitals and healthcare offices on its website. The U.S. Government Accountability Office (GAO) releases reports regarding cyberattacks and data breach in government agencies. There is no standardized system as of yet for recording information thefts in academia. As official records are scattered and underwhelming, this dissertation adopts public media resources for a more complete record of information theft. Two such sources are The Open Security Foundation (OSF) and Identity Theft Resource Center (ITRC), both non-profit organizations, who release data breach incidents which they collect from public media and selected State Attorney General's offices. These data breach reports are commonly used for the analysis of information theft by researchers both academic and professional.

4.5.1. Main Sources for Information Theft Incidents

4.5.1.1. Open Security Foundation (OSF)

The Open Security Foundation (www.datalossdb.org) is a non-profit organization that collects articles and documents pertaining to data breach incidents. This database posts the date of incident release, name of organization, type of incident, summary of incident, date of breach, date of discovery, date of victim notification, location of victim, and other financial information pertinent to organizations involved in each breach.

4.5.1.2. Identity Theft Resource Center (ITRC)

The Identity Theft Resource Center (ITRC) is a non-profit organization that collects case information of identity thefts and data breaches from newspaper articles, televised news, selected state Attorney Generals' offices, blogs, and other open resources. The ITRC posts data breach reports every month.

4.5.1.3. U.S. Department of Health and Human Services

The U.S. Department of Health and Human Services collects information theft data in medical institutions and displays it at the following URL:

(http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html). This website provides information related to data breaches which affect more than 500 individuals in medical institutions. Included are names of medical organizations, state, numbers of victims, date of incident, type of incident, and location of incident.

4.5.2. Additional Sources for Information on Organizations

4.5.2.1. Manta Database (http://www.manta.com/)

“Manta” is an open web-based database providing information on businesses both large and small, unlike OneSource which only covers larger businesses. This database was used as a supplementary resource to OneSource’s database.

4.5.2.2. 2012 College Handbook

The College Handbook is a reference guide published annually by the College Board. The 2012 edition of this guide includes detailed information on 2,200 four-year colleges and universities and 1,700 two year colleges. Contents include a general profile of accredited institutions, freshman class profiles, selection standards, annual costs, financial aid information, academics, majors, campus computing, and student services.

4.5.2.3. 2012 AHA (American Health Association) Guide

The American Health Association Guide includes comprehensive hospital information compiled from the AHA’s annual survey of the healthcare industry. This resource provides information on 6,500 U.S. hospitals and 4,800 other healthcare institutions. Hospital profiles include organizational structure and hospital demographics such as hospital bed size data, admissions, census, and outpatient visits.

4.5.2.4. U.S. Census

The U.S. Census website (http://www.census.gov/) is maintained by the Census Bureau, a division of the Department of Commerce. It provides comprehensive data on people, businesses, and geography in the United States. Numbers of employees in government organizations as used in this research were collected from this source. Some size information for business organizations are also collected from this source.

4.5.2.5. U.S. Office of Personal Management

The U.S. Office of Personal Management (http://www.opm.gov/index.asp) provides comprehensive data on federal government employees. The numbers of federal employees as they appear in this dissertation were collected from this source.

4.6. Descriptive Data

The total number of data and information theft incidents identified in four types of organizations is 1,895 based on the primary databases consulted for this research, the Open Security Foundation (OSF) and Identity Theft Resource Center (ITRC). Among the 1,895 incidents, 1,114 incidents are hacking and 781 incidents are insider theft. More descriptive data is available in Table 9. Those incidents are reported from 2007 to 2013.

Table 9: Descriptive Information Theft Data in 2007-2013

	Business	Education	Healthcare	Governmental	Total
Hacking	758	171	61	124	1,114
Insider Theft	412	22	196	151	781
Total	1,170	193	257	275	1,895

4.7. Data Analysis Limitations

According to Newman and McNally (2005), there is a “lack of solid research examining identity theft, and the research that does exist suffers from numerous data-related and methodological limitations.” There are no complete databases dealing with data breach or identity theft maintained by law enforcement agencies in the United States. While public media sources offer more meticulous databases, they are by no means complete themselves. Accordingly, the data used here was not able to show the full scale of information theft. Again, this is usually because organizations suffering information theft only sustain further losses by sharing news of a crime. A direct survey of organizations which experienced information theft would be extremely useful for this research. However, in surveys related to cybercrime, the response rates rarely exceed 4 or 6% (See Table 7). More often than not, apart from fearing damage to market shares and reputation, organizations simply don’t have the requested information.

Chapter Summary

This chapter explains the research design of this dissertation. Based on the Rational Choice and Situational Crime Prevention theories, research questions and hypotheses are developed for examining the environmental factors of information theft. Different types of organizations are assumed to experience different frequencies of information theft, and have differing detection time periods. The unit of analysis is the amount of information thefts. The dependent variable is the rate of hacking and insider theft. Incident rates were calculated by dividing reported incidents at each industrial sector by total firms per those sectors. Independent variables are types of organizations, employee numbers, and detection time periods. Data for this research is collected from: the Open Security Foundation, Identity Theft Resource Center, and Department of Health and Human Services. Additional sources of information are the Manta database, 2012 College Handbook, 2012 American Health Association Guide, U.S. Census, and Office of Personal Management. 1,895 cases are collected in total. Among them, hacking incidents account for 1,114 cases and insider theft for 781 cases. Limitations of this data include all original sources of the data being from public media, which has the potential of being sensationalist, and a lack of detail.

CHAPTER 5: Analyses and Results.

5.1. Descriptive Statistics of Information Thefts in Business

Where business is concerned, a total of 1,170 incidents of information theft, hacking and insider theft, were identified from the databases of the OSF and ITRC during 2007-2013. Among the 1,170 incidents, 758 incidents were hackings (64.8%) and 412 incidents were insider thefts (35.2%). The most common targets were retail and wholesale stores, which account for 213 of the recorded incidents. The next most common targets are financial service providers, banks, and food service places, in that order. Total 347 incidents (29.7%) are reported in financial service sector. Table 10 provides a detailed summary of how the 1,170 hacking and insider theft incidents are distributed.

Table 10: Descriptive statistics of information theft incidents by business sectors in 2007-2013.

Category	Industrial Sector	Incident Frequency		
		Total	Hacking	Insider theft
Financial Service	Financial Service	135	88	47
	Bank	127	66	61
	Insurance	60	29	31
	Tax service	25	11	14
IT Related Service	Telecommunications	51	25	26
	Data Service	51	44	7
	Publishing/Web Service	44	43	1
	Broadcasting/Media	19	13	6
General Business Service	Retail/Wholesale Stores	213	159	54
	Food Service	124	73	51
	Manufacturing	102	77	25
	Professional Service	86	56	30
	Hotel	49	37	12
	Transportation	14	8	6
	Administrative Support	31	18	13
	Car Dealer	14	2	12
	Energy	13	7	6
	Gas station	12	2	10
	Total	**1,170**	**758**	**412**

Sources: Compiled from ITRC and OSF in 2007-2013.

5.2. Descriptive Statistics of Information Thefts in Education

As stated, research on information theft in colleges and universities is scarce. In places of higher learning, the frequency gap between hacking and insider theft is wide, with hacking being the overwhelming source of information theft. Of 193 reported information thefts targeting colleges or universities, 171 incidents (88.6%) were committed by hacking incidents (See Table 11).

Table 11: Information thefts at colleges and universities in 2007-2013.

Type	Total incident	Hacking	Insider Theft	Total Colleges/ Universities
Colleges/ Universities	193 (100%)	171 (88.6%)	22 (11.4%)	4,599

5.3. Descriptive Statistics of Information Thefts in Healthcare

Medical organizations account for hospitals where providing comprehensive medical treatments to patients and maintain staffed beds, medical clinics with the purpose of providing limited healthcare directly to outpatients, and healthcare businesses where providing supportive services to hospitals and medical clinics. Data of the numbers of employees were collected from U.S. Census of 2012, American Health Association, and “Manta” web source. There are a total of 5,723 hospitals in the United States as of 2013 (AHA, 2014). The national average number of employees at hospitals is 861 (U.S. Census, 2012). There are total 431,305 medical clinics/facilities (U.S. Census, 2012). The national average numbers of employees at those facilities were 13. Healthcare businesses provide the services of medical laboratory analyses, home care, nursing home, rehabilitation, physical therapies, and medical supplies. The counted number of healthcare businesses is 211,258 as of 2012.

Based on the sources of this research, 257 hacking and insider theft were identified in healthcare institutions from 2007 to 2013. Among them, 160 incidents took place in hospitals, 74 in medical clinics and 23 in healthcare businesses (See Table 12).

Table 12: Reported Incidents in Medical Organizations in 2007-2013

	Total	Hacking	Insider Theft	Total Facilities
Hospitals	160	25 (41%)	135 (68.9%)	5,723
Clinics	74	26 (42.6%)	48 (24.5%)	431,305
Healthcare	23	10 (16.3%)	13 (5.6%)	211,258
Total	257	61 (100%)	196 (100%)	

Source: Compiled from ITRC, OSF, U.S. Census, AHA guide, and Manta website.

As visible from the Table 12, insider theft in hospitals is the most common form of information theft in medical organizations overall. Overall, insider theft in medical organizations are more found compared to hacking incidents. The Chi-square test found that there was statistical difference between incident types, hacking and insider theft, and organizational types, hospitals, clinics and healthcare (χ^2 (5) = 258.9, p<.01).

5.4. Descriptive Statistics of Information Thefts in Government

The U.S. government is a popular target for foreign hackers because of political motivations as well as the fame offered by successfully breaching government networks. Government agencies produce and maintain a wide range of data and information. At present, there are 478 federal agencies, 51 state governments (including the District of

Columbia), 289 city governments for cities with populations of at least 100,000, and 73,727 municipal/local governments in the United States. Table 13 shows a detailed outline of this information.

Table 13: Categories of Governmental Organizations

Category	Federal	State	City	Municipal/Local
Type of organization	Federal	State	City with more than 100,000 population	- County - Town - City with less than 100,000 population
Total numbers of organization	478	51 (D.C. included)	289	73,727

Source: U.S. Census (2012).

As reported from the databases of ITRC and OSF during 2007-2013 period, information thefts, hacking and insider theft, are frequently reported by state governments (40.7%) than any other level government. Hacking incidents are more recorded in state-level governments among other types of governments (37.1%). Insider theft incidents are also more reported in state-level governments (43.7%) (See Table 14).

Table 14: Information Thefts in Governmental Organizations (N=275)

Type	Total	Hacking	Insider Theft
Federal	66 (24%)	31 (25%)	35 (23.2%)
State	112 (40.7%)	46 (37.1%)	66 (43.7%)
City	37 (13.5%)	15 (12.1%)	22 (14.6%)
Municipal/Local	60 (21.8%)	32 (25.8%)	28 (18.5%)
Total	275 (100%)	124 (100%)	151 (100%)

Source: Compiled from ITRC, OSF, and U.S. Census.

5.5. Hypotheses Testing

This research provides a detailed analysis of information theft while exploring the differing rates of hacking and insider theft in four types of organizations. In order to demonstrate the statistical difference between outsider hacking and insider theft across organization types, the Chi-square tests and Mann-Whitney test are used on non-parametric data from the adopted database. To explore the time period differences of detecting the incidents among the examined organizations, the Chi-square tests are performed due to the fact that the data for detection time period is also non-parametric data. Lastly, the Chi-square tests for statistical differences in the seasonal variations among the four organizations are used.

5.5.1. Test for the Incidents by Size

Hypothesis Tests	
H1	**Hacking incidents are more likely to occur at smaller organizations.**
H2	**Insider theft incidents are more likely to occur at larger organizations.**

5.5.1.1. Test for determining the incidents by size in business organizations

Based on the above data in Table 13, this research examines how a business’s size influences whether it is more vulnerable to hacking or insider theft. It is natural to assume that a larger organization will create more vulnerabilities and, accordingly, bring more opportunities for offenders. As outlined in Chapter Four, the size is determined by number of employees and branch in business sector. Due to limited data, entire listing of employees and branch offices from identified victim businesses is not available. The employee numbers are counted from the entire branch firms and headquarters which a top parent firm operates across the United States. This research assumes that a business firm will operate the unified standards and manuals for IT security management across entire branch offices. Therefore, the entire employee size is a more standardized factor to determine the size of an organization. For Table 14, the average firm employees of any given industrial sector are calculated by dividing the total sum of employees counted in those incident-affected business firms by the number of incident-affected business firms in that sector. Those employee size are calculated by the type of incident, hacking and insider theft. The data characteristics in the examined business sectors are non-parametric. Therefore, the Chi-square tests are performed to determine statistical differences between the average employee numbers and incident types. Those outcomes are presented in the table 15.

Table 15: Average Employees of victim business by incident type

Category	Industrial Sector	Average firm employees		Size Comparison (Larger)	Chi-Square Test
		Hacking (N=549)	Insider Theft (N=261)		
Financial Service	Bank	27,925	50,288	Insider	$\chi^2(1)=6{,}394.13$, *p* <.001.
	Insurance	15,392	33,167	Insider	$\chi^2(1)=6{,}506.53$, *p* <.001.
	Financial Service	7,530	8,333	Insider	$\chi^2(1)=40.65$, *p* <.001.
	Tax service	1,262	443	Hacking	$\chi^2(1)=393.41$, *p* <.001.
IT Related Service	Telecommunications	31,233	57,645	Insider	$\chi^2(1)=7848.9$, *p* <.001.
	Data Service	27,057	35,254	Insider	$\chi^2(1)=11{,}046.1$, *p* <.001.
	Publishing/Web Service	2,528	21,500	Insider	$\chi^2(1)=14{,}979.9$, *p* <.001.
	Broadcasting/Media	22,178	10,507	Hacking	$\chi^2(1)=4{,}167.4$, *p* <.001.
General Business Service	Retail/Wholesale Stores	15,627	87,532	Insider	$\chi^2(1)=50{,}120$, *p* <.001.
	Manufacturing	13,281	38,781	Insider	$\chi^2(1)=12{,}490$, *p* <.001.
	Transportation	6,541	21,712	Insider	$\chi^2(1)=8{,}146.4$, *p* <.001.
	Energy	1,421	6,513	Insider	$\chi^2(1)=3{,}268$, *p* <.001.
	Food Service	1,205	5,353	Insider	$\chi^2(1)=2{,}623.7$, *p* <.001.
	Administrative Support	845	5,024	Insider	$\chi^2(1)=2{,}975.6$, *p* <.001.
	Hotel	968	831	Hacking	$\chi^2(1)=10.4$, *p* <.01.
	Professional Service	1,256	614	Hacking	$\chi^2(1)=220.4$, *p* <.001.

The test outcomes indicate that insider theft occurs most commonly in banks, insurance companies, financial business firms, communications/media companies, data services, publishing/web service, retail/wholesale stores, manufacturers, transportation, energy, restaurants, and general administrative companies where larger employee sizes are found compared to hacking-affected business sectors, tax services, broadcasting services, hotels, and professional services. Smaller business organizations may have limited resources for maintaining their IT security managements. Because larger business firms have a larger size of employees, there might be limitations to supervising the entire staff including full-time and part-time employees working on business travelling, on at their home, and on frequent work-shifts, accounting for insider theft being more common in those environments

5.2.1.2. Test for determining the incidents by size in educational organizations

Colleges and universities including graduate schools targeted by hackers have an average size of 18,158 students, and are considered to be large. Colleges and universities experienced the insider theft are those with an average size of 14,453 students or less (see Table 16). In educational sector, colleges and universities are only one sector to compare. The data of hacking and insider theft in the examined educational institutions are non-parametric. For this reason, this research adopts a Mann-Whitney Test for comparing the organizational sizes between hacking and insider theft in higher educational institutions.

Hacking incidents (Mdn=13,533) are more found at colleges and universities with larger students compared to insider thefts (Mdn=11,991), *U*=4,625,613, p<.001, r=-1.28. Larger universities are maintaining more information and data including scientific researches collaborated with high-technology intense companies. Hackers may find more opportunities in these places.

Table 16: Incident Type by Organization Size in Colleges/Universities.

	Organization Size by Average Students					
	Hacking (N=171)			Insider Theft (N=22)		
Category	**Mean**	**Max**	**Min**	**Mean**	**Max**	**Min**
Colleges/ Universities	18,158	54,833	403	14,453	39,029	1,772

Source: Compiled from College Handbook 2012.

5.5.1.3. Test for determining the incidents by size in medical organizations

The available data was applied to one of hypotheses that insider theft targeting medical organizations more occurs in large hospital. With the Chi-square tests, findings support that hypothesis: insider thefts were found more frequent at larger hospitals an average of 5,018 employees, $\chi^2(1)=171.5$, $p <.001$. Hacking mostly targets hospitals with averages of 3,789 employees. In medical clinics, insider thefts commonly occur at offices with an average of 41 employees, while hackings commonly target clinics with an average of 15 employees, $\chi^2(1)=12.1$, $p <.01$. In healthcare businesses, insider thefts are reported with an average of 1,348 employees, and hackings are reported with an average of 4,470 employees, $\chi^2(1)=14{,}699.5$, $p <.001$. (See Table 17). Healthcare business are showing a different outcome compared to hospitals and clinics. Insider thefts are more common at small scale healthcare services. Due to lack of supervision, insider offenders may cover their offenses.

Table 17: Incident Types by Organizational Sizes at Medical Organizations

	Organization Size by Average Employees					
	Hacking			Insider Theft		
Category	**Mean**	**Max**	**Min**	**Mean**	**Max**	**Min**
Hospital	3,789	9,794	30	5,018	17,243	156
Clinics	15	100	2	41	175	2
Healthcare	4,470	18,375	4	1,348	3,800	4

Source: Compiled from OSF, ITRC, AHA Guide and Manta website.

Because larger hospitals have so many employees, there might be limitations to supervising the entire staff when there are other matters of life and death to attend to or where there are frequent work shifts around the clock, accounting for insider theft being more common in those environments.

5.5.1.4. Test for determining the incidents by size in governmental organizations

The size for governmental organizations is determined by the type of government in this research. Federal governments are categorized as large sized organization. Due to the complexities and variances of size and functions for state and city governments, those two types of organizations are categorized as medium sized organization. Lastly, municipal and local governments are categorized as small sized organization in governmental types.

Federal, state, city, and municipal/local governments experienced 31, 46, 15 and 32 hacking cases, respectively (See Table 14). There is a statistical difference between types of governmental organizations and hacking incidents, χ^2 (3) =15.55, *p* <.01.

For the insider theft case, federal, state, city and municipal/local governments showed 35, 66, 22 and 28 incidents, respectively. The inside theft incidents are also showing a statistical difference between types of governmental organizations and insider theft incidents, χ^2 (3) =30.43, *p* <.01.

5.5.2. Test for the Information Theft Rates

Hypothesis Tests	
H3	**Governmental organizations will likely experience higher rates of information theft.**

To test this hypothesis, this research identified the total incidents of information theft at each industrial sector. Then those incident numbers by hacking and insider theft are divided by the total numbers of firms at each industrial sectors and multiplied by 100. The total firm numbers of each industrial sector are presented in Appendix I.

For calculating the incident rates of state governments, this research counted the numbers of states which experienced hacking and insider theft and those numbers of states are divided by total numbers of states, 51. The numbers of states which experienced hacking and insider theft are 39 and 24 states, respectively. However, the total numbers of states which experienced hacking or insider theft are 44 among 51 states.

State governments record the highest rate of incident (86.27) among other governmental organizations. Federal governments record the second highest incident rate of 13.78. City governments record the rate of 12.8. Municipal/local governments show the lowest incident rate of 0.16 among governments (See Table 18).

Average hacking incident rate of state governments is 76.5, federal 6.472, city 5.19 and municipal/local 0.083, respectively. For the insider theft case, federal, state, city and municipal/local governments showed 35, 66, 22 and 28 incidents, respectively.

Overall governmental sectors including federal, state, city governments are showing higher rates of information theft compared to business, educational and medical organizations. U.S. governments are collecting a variety of information form the citizens and their organizational structures are complex. Those federal, state, city and municipal governments are symbolic entities to represent the values of the United States. Therefore, there may be more opportunities, motivations and vulnerabilities in the U.S. governments for offenders.

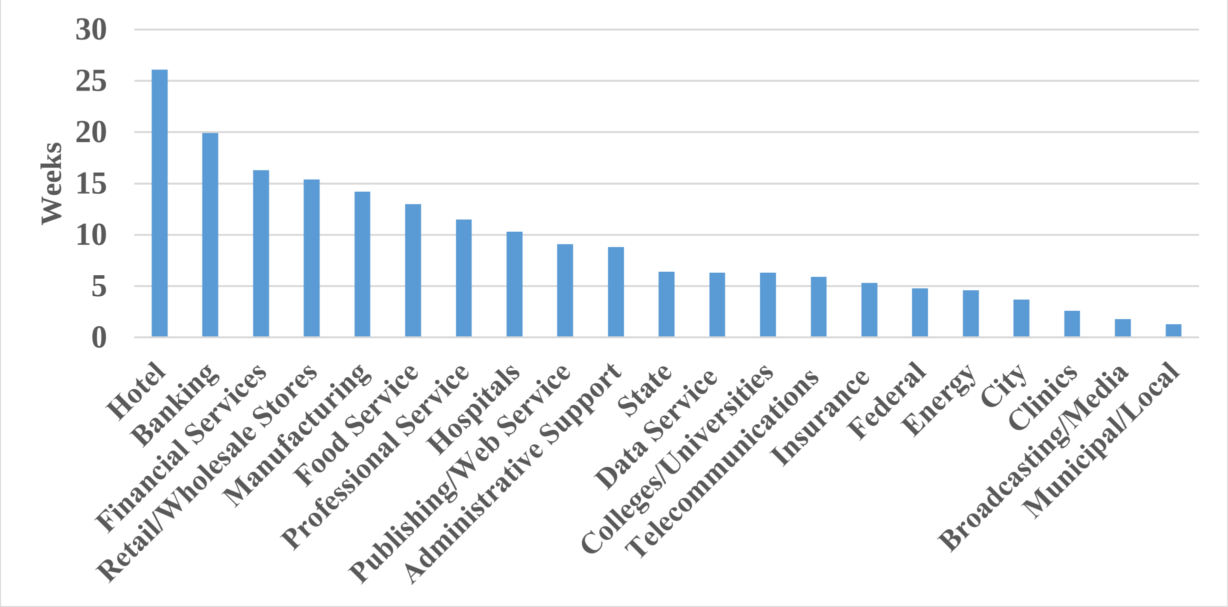
Table 18: Information theft rates by industrial sector

Sector	Total Incident Rates	Sector	Hacking Rate	Sector	Insider Rate
State	86.27	State	76.500	State	47.100
Federal	13.78	Federal	6.472	City	7.612
City	12.80	City	5.190	Federal	7.307
Hospital	4.58	Higher Education	3.718	Hospital	2.359
Higher Education	4.20	Bank	0.490	Higher Education	0.478
Bank	0.94	Data Processing	0.459	Bank	0.453
Tele-communications/ Internet Service	0.59	Hospital	0.440	Tele-communications/ Internet Service	0.303
Data Processing	0.53	Tele-communications/ Internet Service	0.291	Broadcasting/Media	0.128
Broadcasting/Media	0.41	Broadcasting/Media	0.278	Utilities: energy	0.103
Financial Service	0.23	Publishing/Web Service/Software	0.156	Financial Service	0.080
Utilities: energy	0.22	Financial Service	0.149	Data Processing	0.073
Publishing/Web Service/Software	0.16	Utilities: energy	0.120	Municipal/Local	0.072
Municipal/Local	0.16	Municipal/Local	0.083	Insurance	0.023
Hotel	0.09	Hotel	0.071	Hotel	0.023
Manufacturing	0.04	Manufacturing	0.030	Car Dealer	0.015
Insurance	0.04	Insurance	0.022	Gas station	0.015
Retail/Whole sale Stores	0.03	Retail/Whole sale Stores	0.019	Tax Service	0.012
Professional Service	0.03	Professional Service	0.019	Food Service	0.011
Food Service	0.03	Food Service	0.016	Medical/Health Service	0.011
Car Dealer	0.02	Tax Service	0.010	Manufacturing	0.010
Gas station	0.02	Administrative and Support Services	0.006	Professional Service	0.010
Tax Service	0.02	Medical/Health Service	0.006	Retail/Wholesale Stores	0.007
Medical/Health Service	0.02	Transportation	0.005	Nursing/Social Service	0.006
Administrative and Support Services	0.01	Nursing/Social Service	0.005	Transportation	0.004
Nursing/Social Service	0.01	Gas station	0.003	Publishing/Web Service/Software	0.004
Transportation	0.01	Car Dealer	0.002	Administrative and Support Services	0.004

5.5.3. Tests for the Detection Time Variations

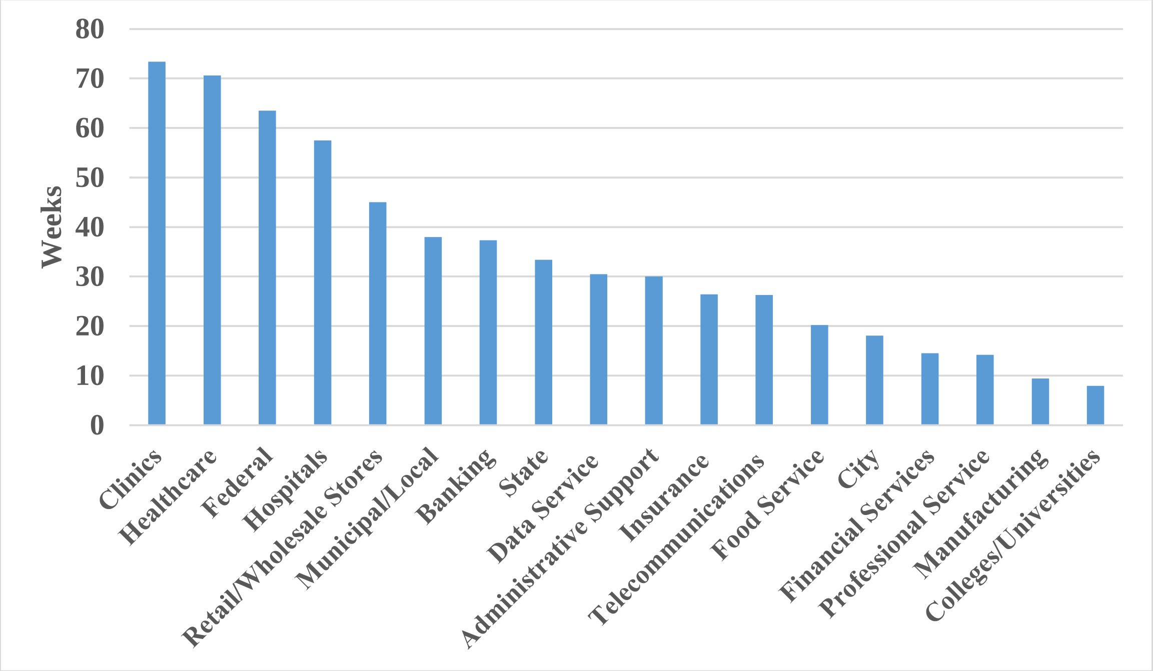
This section examined which organization would detect their information theft incidents more quickly compared to other types of organizations.

Figure 3: Detection time periods (weeks) of hacking incidents by industrial sectors



Across all industrial sectors, detection time periods in hacking incident are found statistically different (χ^2 (20) =87.4, *p =.00* <.01). Financial sector including banking and general financial services tends to take a longer time to detect hacking incidents compared to other industrial sectors (See Figure 3).

Figure 4: Detection time periods (weeks) of insider theft by industrial sectors



Across all industrial sectors, detection time periods in insider theft are found statistically different (χ^2 (19) =278.285, $p = .00 < .01$). Medical sector and federal governments tend to take a longer time to detect insider theft incidents compared to other industrial sectors (See Figure 4).

5.5.3.1. Detection time period of information theft incidents in business organizations

For the analysis of detection time period, incident cases below five per industrial sector are excluded. Transportation and Tax service sectors are excluded. In business organizations, detection time period, how long it takes an organization to detect that they've been stolen from information theft, is longer for insider thefts, particularly at retail and wholesale stores (45 weeks), banks (37.3 weeks), data service (30.5 weeks), administrative service (30 weeks), insurance (26.4 weeks), telecommunications (26.3 weeks) and food services (20.2 weeks) (See Table 19).

For hacking incidents, hotels take a longer time to detect the incident (average 26.1 weeks). Banking, financial services, retail/wholesale stores, and manufacturing sectors are also take longer time to detect the hacking incidents, 19.9, 16.3, 15.4, and 14.2 weeks, respectively. The detection time periods for hacking and insider theft at each business sector are of significant difference (hacking χ^2 (13) =50.58, *p*<.01; and insider theft χ^2 (10) =58.17, *p*<.01), as per outlined in Table 19.

Table 19: Detection time period of hacking and insider theft by week

Category	Industrial Sector	Average Weeks Until Detected					
		Hacking (N=330)			Insider theft (N=138)		
		Mean	Max	Min	Mean	Max	Min
Financial Service	Banking	19.9	108	1	37.3	104	1
	Financial Services	16.3	87	1	14.5	70	1
	Insurance	5.3	13	1	26.4	67	1
IT Related Service	Telecommunications	5.9	20	1	26.3	61	4
	Data Service	6.3	18	1	30.5	79	1
	Publishing/Web Service	9.1	30	1	na	na	na
	Broadcasting/Media	1.8	5	1	na	na	na
General Business Service	Retail/Wholesale Stores	15.4	129	1	45	184	1
	Food Service	13	34	1	20.2	88	1
	Manufacturing	14.2	116	1	9.4	32	1
	Professional Service	11.5	38	1	14.2	43	1
	Hotel	26.1	110	1	na	na	na
	Administrative Support	8.8	31	1	30	87	4
	Energy	4.6	12	1	na	na	na
	Gas station	na	na	na	7.5	24	1
Average Weeks		11.3			23.8		
Chi-square Test		χ^2 (13) =50.58, p<.01			χ^2 (10) =58.17, p<.01		

Source: Compiled from the databases of OSF and ITRC.

5.5.3.2. Detection time period of incidents in higher educational organizations.

The detection time periods for hacking and insider theft are rather short, 6.3 and 7.9 weeks respectively, compared to other industrial sectors. Those two types of information theft at colleges and universities are of no significant difference (χ^2 (1) =2.515, p>.05), as per outlined in Table 18. However, the available samples of insider theft in higher educational organizations are small (N=7). Further research with more samples is needed.

Table 20: Average time until detected for information theft in educational organizations

	Detection Time Period by Average Weeks					
	Hacking			Insider Theft		
	Mean	Max	Min	Mean	Max	Min
College/ Universities	6.3 (N=78)	100	1	7.9 (N=7)	24	1

5.5.3.3 Detection Time Period of Incidents in medical organizations

Regarding detection time periods of information thefts in hospitals, insider theft takes longer to detect, an average of 57.5 weeks, compared to hacking, which takes an average of 10.3 weeks. Insider theft incidents at clinics also remain undetected longer; 73.4 weeks on average versus a detection time of 2.6 weeks to detect hacking incidents. Insider theft in healthcare businesses remains undetected for a mean of 70.6 weeks. However, since samples of hacking incidents in healthcare businesses are small (N=3) and are excluded for the analysis. Hacking incidents do not show statistical difference in the detection periods among medical organizations (χ^2 (1) =3.77, p=.052 >.05). Insider theft incidents also do not show statistical difference in the detection periods among medical organizations (χ^2 (2) =1.97, *p*=.373>.05) (See Table 21).

Table 21: Detection Time Period by Medical Organizational Types

	Detection Time Period by Average Weeks					
	Hacking			**Insider Theft**		
	Mean	**Max**	**Min**	**Mean**	**Max**	**Min**
Hospital	10.3 (N=52)	54	1	57.5 (N=52)	259	1
Clinics	2.6 (N=7)	10	1	73.4 (N=18)	220	2
Healthcare	na	na	na	70.6 (N=13)	180	1
Average Week	6.5			67.17		
Chi-square Test	χ^2 (1) =3.77, *p*=.052 >.05			χ^2 (2) =1.97, *p*=.373>.05		

Source: Compiled from OSF, ITRC, U.S. Census, AHA guide and Manta website.

5.5.3.4. Detection Time Period of Incidents in governmental organizations

Table 25 shows the differences in detection periods for hacking and insider theft among the four types of governmental organizations. State governments typically detect hacking incidents in about 6.4 weeks. However, hacking incidents do not show statistical difference in the detection periods among four types of governments (χ^2 (3) =3.5, p>.05). Federal agencies take an average of 63.5 weeks to detect insider theft. Data indicates there is a significant discrepancy between the detection periods of different levels of government in insider theft incidents (χ^2 (3) =28.8, p=.00<.01) (See Table 22).

Table 22: Detection Period by Governmental Organizational Types (N=84).

	Detection Time Period by Average Weeks					
	Hacking			Insider Theft		
	Mean	Max	Min	Mean	Max	Min
Federal	4.8 (N=9)	17	1	63.5 (N=10)	199	10
State	6.4 (N=20)	45	1	33.4 (N=12)	130	1
City	3.7 (N=6)	13	1	18.1 (N=7)	47	1
Municipal	1.3 (N=11)	3	1	38 (N=9)	105	2
Average Weeks	4.1			38.3		
Chi-square test	χ^2 (3) =3.5, p=.321>.05			χ^2 (3) =28.8, p<.01		

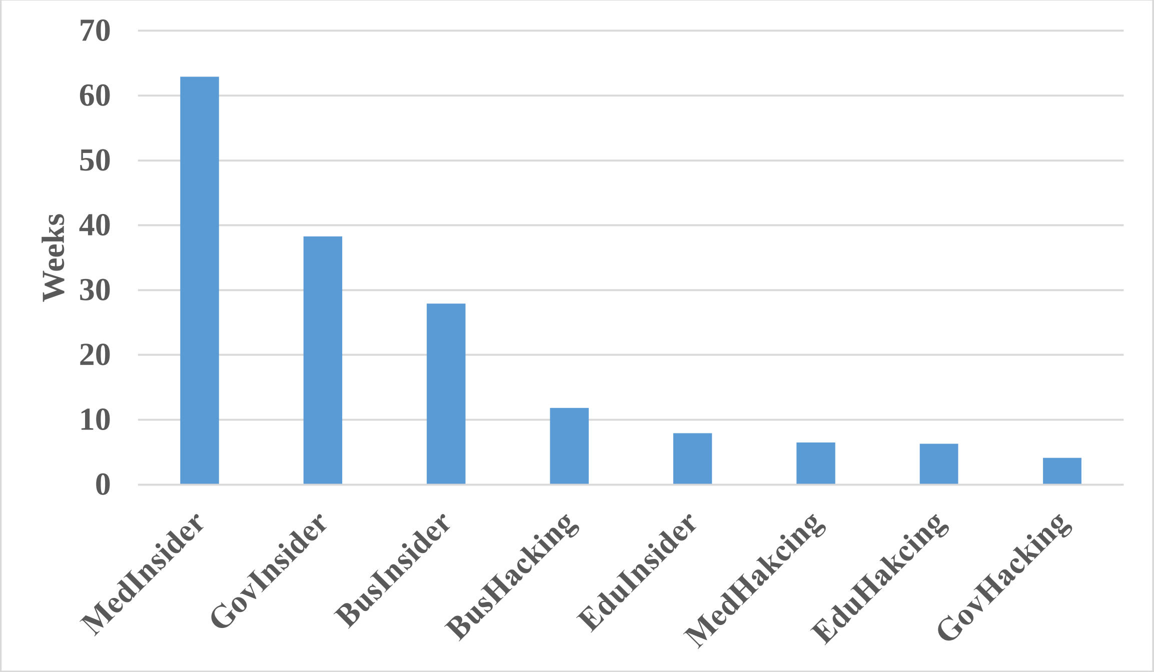
5.5.4. Test for the Detection Time Period for Insider Theft

Hypothesis Tests	
H4	**Insider theft incidents will take a longer time to detect.**

To test this hypothesis, incident detection time periods at each industrial sector in four types of organizations are examined. Then average weeks of detection time period of hacking and insider at each industrial sectors are calculated. Data of detection time period in hacking incidents is non-parametric and data of insider theft is non-parametric as well.

First, to test overall differences of detection time periods between hacking and inside theft incidents, the Mann-Whitney test is performed. Insider theft incidents over four types of organizations (Mdn=22) are significantly longer to detect than hacking incidents (Mdn=4), U=33,185.5, p<.001, r=-.39.

Figure 5: Detection time periods for hacking and insider theft by organizations



In the second step, for analyzing the detection time differences by organization and type, this research tried to identify a proper statistical test. Since the data of detection time periods is non-parametric and the equal variances of the detection time period data in four types of organization are not assumed, a oneway-ANOVA or a Kruskal-Wallis tests for comparing groups with more than two are not adopted for testing this hypothesis. Therefore, this research performed a Chi-square test for determining whether there are significant differences between the mean weeks of detection time period by hacking and insider theft incidents. Upon the Chi-square test analysis, the difference between these variables was significant, χ^2 (7) =147.54, p<.001. Insider theft in medical organizations takes the longest time to detect the insider theft (62.9 weeks). Government organizations take a shorter time to detect the hacking incidents compared to other organizations (4.1 weeks).

5.5.5. Tests for the Detection Time Period by Governments

Hypothesis Tests	
H5	**Governmental organizations will detect the information theft more quickly.**

Governmental organizations are assumed to maintain a higher level of IT security management because those organizations are handling a variety of information including national security related information. Foreign hackers are targeting symbolic federal organizations. For testing this hypothesis, incident detection time periods at each industrial sector in four types of organizations are also examined. Then average weeks of detection time period are calculated.

Since the data of detection time periods is non-parametric and the equal variances of the detection time period data in four types of organization are not assumed, a oneway-ANOVA or Kruskal-Wallis tests are not adequate for testing this hypothesis. Therefore, this research performed a Chi-square test for comparing the mean weeks of detection time period for insider theft incidents in four types of organizations.

A chi-square test of equality was performed to examine the relation between types of organization and mean weeks of detection time period for insider theft. The relation between these variables was significant, χ^2 (3)=45.71, N=267, p<.01. Mean weeks of detection time period of insider theft are in higher education and business organizations are shorter to detect the insider theft than medical and governmental organizations.

Separately, the second chi-square test of equality was performed to examine the relation between types of organization and mean weeks of detection time period for hacking incident. The relation between those variables was not significant, χ^2 (3)=45.14, N=513, p>.05. Mean weeks of detection time period of hacking incident in four types of organizations are not statistically different.

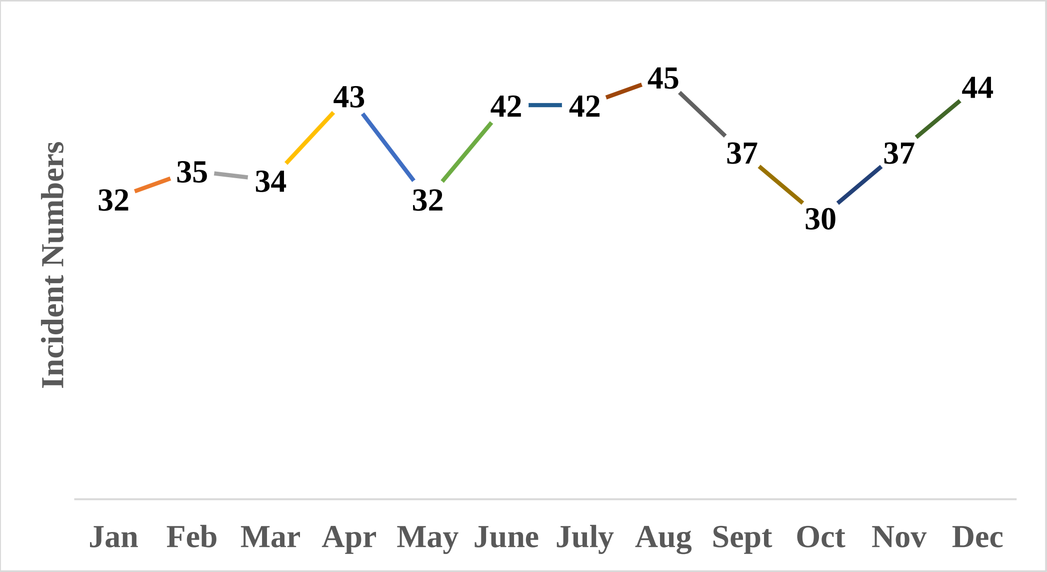
5.5.6. Tests for the seasonal variation

Hypothesis Tests	
H6	**Information theft incidents are not likely to show seasonal variation.**

There are several studies suggesting seasonal patterns in property crime. (Block, 1983; BJS, 1988; Hurd and Ruparel, 2007, and Lauritsen and White, 2014). However a seasonal variation in information theft, hacking and insider theft, has not yet been established. Because the internet is easy to access and employees at organizations are directly working with the data and information, it is assumed that no particular time of the year is more suited to cyber hacking insider theft than other traditional types of offenses. This dissertation explores whether or not such a seasonal variation can be found in information thefts that targets four types of organizations. For determining seasonal variation, information theft cases during each month from 2007- 2013 are analyzed; a total of 666 cases with available information about the time of incident occurrence. In the search for monthly variations, all incident cases were counted by each month. Statistical significance of difference for those accumulated frequencies of incidents was assessed by a Chi-square test in four types of organizations separately. The tests revealed no significant statistical difference between the time of the month and number of hacking incidents at that time in business, medical, and governmental organizations. Educational organizations only showed a statistical difference between the monthly time and number of hacking incidents.

5.5.6.1. Seasonal Variation in Hacking Incidents

Figure 6: Seasonal Variation of Hacking Incidents in 2007-2013

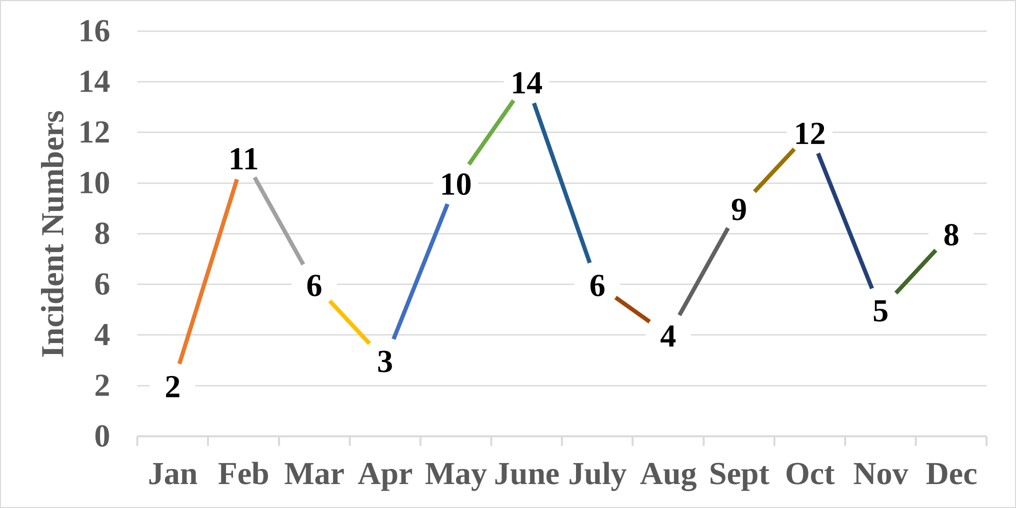


Source: Compiled from reports by the ITRC and OSF

In business sector in general, hacking incidents (N=453) did not show a statistical significance of difference by each month ((χ^2 (11) = 8.06, *p* =.708>.05) (See Figure 6). In medical organizations, hacking incidents (N=41) which were counted in hospital, medical clinics and healthcare sectors did not show a statistical significance of difference by each month ((χ^2 (11) = 6.707, *p* =.822<.05). In governmental organizations, hacking incidents (N=79) which were counted in federal, state, city and municipal levels did not show a statistical significance of difference by each month ((χ^2 (11) = 5.911, *p* =.879<.05).

The chi-square test for educational organizations, colleges and universities reveals a monthly frequency difference in hacking incidents (N=93) for the given time frame in 2007-2013 ((χ^2 (11) = 26.355, *p* =.006<.01). Unlike in business, medical and governments, hacking incidents in education do in fact show seasonal variations. February, June, and October are the most common months where (11, 14, and 12, respectively). Naturally, hacking is most common while higher educational institutions are in session. Figure 6 below outlines these variations in more detail.

Figure 7: Hacking incidents at higher educational organizations in 2007-2013



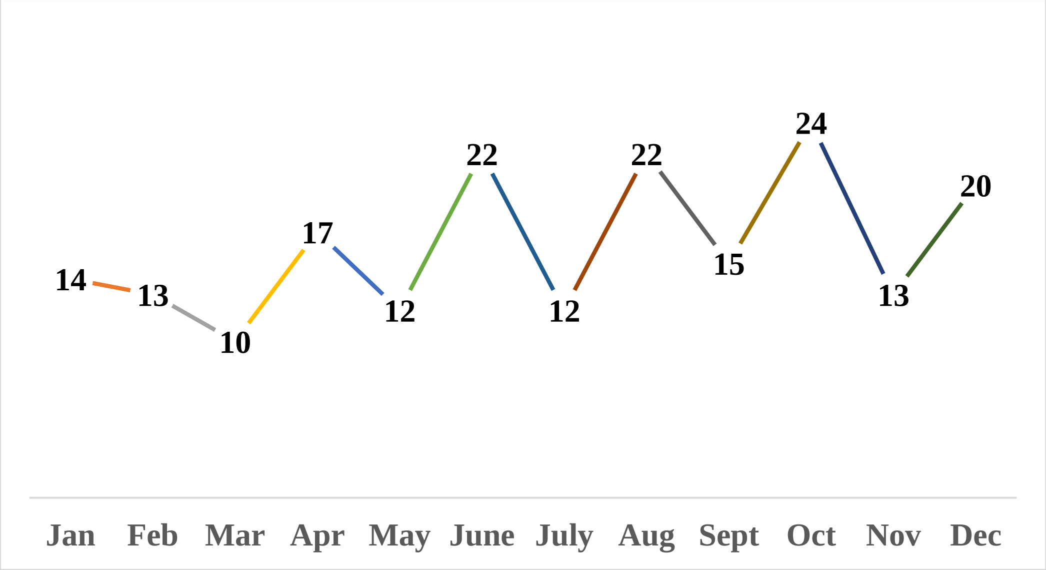
Source: Compiled from reports by the ITRC and OSF

5.5.6.2. Seasonal Variation in insider theft

This dissertation also explores whether or not any seasonal variation can be found in information theft by employees in business, medical and governmental organizations. Due to a lack of data (N=7), higher educational organizations are excluded for this analysis. For determining seasonal variations, a total of 336 cases with available information about the time of incident occurrence are used. As in the same method for assessing the hacking incidents, insider theft incident cases were counted by each month. Then, statistical significance of difference for those accumulated frequencies of incidents was assessed by a Chi-square test in three types of organizations separately. The tests revealed no significant statistical difference between the time of the month and number of hacking incidents at that time in business, medical, and governmental organizations.

In business sector in general, insider theft incidents (N=194) did not show a statistical significance of difference by each month ((χ^2 (11) = 15.072, p=.179>.05) (See Figure 8). In medical organizations, insider theft incidents (N=84) did not show a statistical significance of difference by each month ((χ^2 (11) = 8.857, p =.635>.05). In governmental organizations, insider theft incidents (N=58) which were counted in federal, state, city and municipal levels did not show a statistical significance of difference by each month ((χ^2 (11) = 9.034, p= .619 >.05).

Figure 8: Insider Theft Incidents at Business Organizations in 2007-2013



5.6. SCAREM Model Analyses

5.6.1. Introduction

As mentioned in Chapter Three, the SCAREM model is used to break down the characteristics of offenses in ecommerce. This research applies the SCAREM Model to explain the characteristics of information theft, specifically hacking and insider theft. Among the six attributes of the SCAREM Model, this dissertation refers to four: “Stealth,” “Reconnaissance,” “Escape,” and “Multiplicity” to explain the hacking incidents. The two other attributes, “Challenge” and “Anonymity,” are not applied due to the limited characteristics of available data. For the insider thefts, five attributes of the SCAREM model except “Stealth” concept are used. “Stealth” was not applied for this portion of analysis because of the limited nature of source data. Below descriptions for the SCAREM model are applied in this research.

Stealth

For the bivariate analysis between hacking rate and SCAREM attributes, the "Stealth" ranking score '1' was given to an incident with an identified hacking method, while a score of '2' was given to an incident with an unknown hacking method. Because insider theft is generally all conducted the same way, "Stealth" does not apply for those crimes.

Challenge

The data used here does not include any information about how much time hackers spent and how many techniques they tried. Therefore, this attribute does not apply to hacking analyses. As for insider thefts, insiders will generally gain access they are not authorized for in order to copy, download, or transfer information they wish to steal, and "Challenge" applies in these situations. "Challenge" score '1' is assigned to an incident purely of unauthorized access. Score '2' is assigned to an incident where data and information are copied or transferred to an unauthorized location.

Anonymity

"Anonymity" is a given on the internet, especially where hacking is concerned. Consistent with the difficulty in determining hackers' identities, no source data of this research mentions uncovering who is responsible for a given hack, so this attribute was not considered in hacking analysis.

Insider theft differs in that sometimes insiders are discovered instantly. "Anonymity" score '1' is assigned to former employees or contractors that commit insider theft. Score '2' is assigned to employers guilty of insider theft. For obvious reasons, current employees are difficult to catch in the midst of insider theft, usually having some degree of job security.

Reconnaissance

"Reconnaissance" is naturally an essential part of hacking. For testing this attribute, Reconnaissance score '1' is assigned to an incident where the organization has any information about the incident's occurrence. Score '2' is assigned to incidents where victim organizations have no information about the occurrence. This attribute applies to insider theft in the same way.

Escape

Naturally, information thieves believe they will complete their crimes without detection, or at least without arrest. "Escape" score '1' is given to an incident if the offense is detected in one to four weeks. A score of '2' is assigned to an incident if the incident is detected in five to 26 weeks. A score of '3' is assigned to an incident if the incident is detected in 27 to 52 weeks. Lastly, a score of '4' is assigned to an incident if the incident is undetected for a year or more. Escape applies equally to insider theft as with hacking.

Multiplicity

Information stolen in a hacking incident can often be used to commit more crimes, especially concerning information stolen from banks. A multiplicity score of '1' is given to stolen personal data and information. A score of '2' is given to stolen financial or medical data. A score of '3' is assigned to an incident where the person responsible is arrested and prosecuted, based on the assumption that information thefts pursued rigorously enough by law enforcement to actually result in arrest are more serious than most. Multiplicity applies to insider theft in the same manner as with hacking. Tables 23 details the methodical application of SCAREM in this research.

Table 23: SCAREM Measures and Coding for Hacking and Insider Theft Incidents

SCAREM Attributes	Hacking		Insider Theft	
	Application	**Scoring Code (Rank Measurement)**	**Application**	**Scoring Code (Rank Measurement)**
Stealth	Method of offense	1. Known hacking method (i.e.,virus/ social engineering). 2. Unknown hacking method.	Not measured	N/A
Challenge	Not measured	N/A	Status of stolen data	1. Data accessed. 2. Data copied or stolen.
Anonymity	Not measured	N/A	Status of offender	1. Former employee or contractor. 2. Employee.
Reconnaissance	Preparedness for an offense	1. Available information of incident occurrence. 2. No information of incident occurrence.	Preparedness for an offense.	1. Available information of incident occurrence. 2. No information of incident occurrence.
Escape	Detection period time	1. 1-4 weeks. 2. 5-26 weeks 3. 27-52 weeks. 4. Beyond one year	Detection time period.	1. 1-4 weeks. 2. 5-26 weeks 3. 27-52 weeks. 4. Beyond one year
Multiplicity	Secondary offense	1. Personal data. 2. Financial/medical data. 3. Arrested/prosecuted by law enforcement.	Secondary offense.	1. Personal data. 2. Financial/medical data. 3. Arrested/prosecuted by law enforcement.

5.6.2. Analyses of SCAREM Model for Information Thefts

5.6.2.1 Bivariate Analysis of Hacking Incidents

The bivariate analysis of variables for SCAREM and the hacking theft rate are presented in Table 24. For all variables, *r* coefficients are negatively or positively significant at the $p < .01$ level. The attribute ‘Reconnaissance’ shows a positive relationship with the hacking incident rate (*r* = .13, p <.01), which indicates that the more preparation is involved in hacking incidents, the more likely it will be successful. The attributes of ‘Stealth,’ ‘Escape,’ and ‘Multiplicity’ have negative correlations with the hacking incident rate (*r* =-.08, - .11 and *r* =- .2, respectively, p < .01), indicating that organizations with higher rates of hacking incidents are vulnerable to the attacks in lower levels of hacking skills, a higher rate of hacking corresponds directly with a lower level of IT security management, and therefore, a longer detection period. Organizations with higher rates of hacking incidents show less frequency of secondary incidents resulting from data lost to hackers.

Table 24: Spearman’s Rho Correlation Analysis for the SCAREM Model of Hacking incidents (N= 1,114)

	Hacking Rate	**Stealth**	**Reconnaissance**	**Escape**	**Multiplicity**
Hacking Rate	1.00				
Stealth	-.08**	1.00			
Reconnaissance	.13**	.06*	1.00		
Escape	-.11**		*	1.00	
Multiplicity	-.19**		.12**	.21**	1.00

** p <.01, * p <.05

5.6.2.2. Bivariate Analysis of Insider Theft Incidents

Application of the SCAREM model to insider theft is shown in Table 25. Insider theft rates were found positively related to the concept of ‘Escape’ (r=.2, p<.01), indicating that the higher the insider theft rate is in an organization, the longer that organization takes to detect insider theft. This result contradicts the dynamic found between hacking incident and ‘Escape,’ and confirms that insider thefts take longer to detect. The attribute ‘Challenge’ is negatively related to the insider theft rate (r= - .1, p<.01), suggesting that the data and information are accessed without a certain level of restrictions by inside employees. The attribute ‘Multiplicity’ is negatively related to the insider theft rate (r=-.11, p<.01). This result indicates that higher frequencies of insider incident are coming from more availability of basic levels of data and information. Those findings will contribute to establish proper policy implementations for safety of data and information.

Table 25: Spearman’s Rho Correlation Analysis for the SCAREM model of insider theft incidents (N= 720).

	Insider Theft Rate	Challenge	Anonymity	Reconnaissance	Escape	Multiplicity
Insider Rate	1.00					
Challenge	-.1**	1.00				
Anonymity			1.00			
Reconnaissance				1.00		
Escape	$.2^{**}$	$.193^{*}$			1.00	
Multiplicity	-.11**	$.122^{*}$	.153*			1.00

** p <.01, * p < .05.

5.6.2.3. Mann-Whitney *U* Test Analysis for SCAREM analysis

Due to the limited characteristics of the data used in this analysis, the multivariate test was not performed with the SCAREM variables. Instead, the Mann-Whitney *U* test was employed to find the character differences between hacking and insider theft incidents. The data characteristics of those two types of incidents are non-parametric. The results of the M-W *U* test are displayed in Table 26. Of the six SCAREM attributes, three were commonly matched: Reconnaissance, Escape and Multiplicity. The test was performed with these three attributes between hacking and insider theft.

Table 26: Mann-Whitney *U* Test for Two groups: Hacking and Insider Theft (N=1,671)

	Theft rate	Reconnaissance	Escape	Multiplicity
Mann-Whitney U	410,330	409,080	43,175	321,014
Wilcoxon W	713,361	1,025,685	169,428	764,225
Z	-1.94	-2.106	-9.525	-2.528
Asymp. Sig. (2-tailed)	.052	.038	.000	.011

Hacking rates are higher than insider theft. However, incident rates between hacking and insider theft are not statistically significant among four types of organizations (*U*=410,330, p>.05). This result indicates that two types of information incidents are commonly found in organizations. In the ‘Reconnaissance’ attribute, insider theft cases do not provide more information about the incident (*U*=409,080, p<.05). This finding imply that insider thefts are difficult to detect and estimate the damages. In the ‘Escape’ attribute, inside theft takes to longer to detect (*U*=43,175, p<.01). In the ‘Multiplicity’ attribute, the information stolen by insiders are more used to commit the second offenses (*U*=321,014, p<.05).

Chapter Summary

This chapter explores the basic characteristics of information theft in the four types of organizations. In business, large banks, insurance companies, communications/media companies, data services, energy companies, manufacturers, restaurants, transportation services, retail food stores, and general consulting companies experience insider theft more frequently than hacking incidents. Contrarily, smaller businesses such as financial companies, tax services, IT services, hotels, advertising companies, and general services experience hacking more frequently.

Incident detection time was found to vary between types of incidents. Insider thefts at banks and finance companies take longest to discover. Data services, restaurants, general retail stores, transportation, and non-financial consulting companies take many weeks more to discover insider theft than they do to discover hacking incidents.

Where medical organizations are concerned, insider thefts are more common at large hospitals/healthcare facilities and also take longer to detect. In education, hacking is exceedingly more common than insider theft. However, while hacking incidents occur more often at large schools, insider theft is more common at smaller schools. In government, hacking and insider theft were both found most common at the state level. The detection time for hacking is also longest for state governments. The detection time for insider theft is longest at the federal level.

Available statistics reveal no seasonal variation in hackings that target businesses. There are seasonal variations for hackings targeting educational institutions, however. Medical and governmental organizations are not included in the analysis of seasonal variations due to a lack of data.

In testing the characteristics of information theft in four types of organizations, the SCAREM model is adopted. Hacking rates are positively related to SCAREM’s element “Reconnaissance” and inversely related to the elements “Escape” and “Multiplicity.” Insider theft rates are inversely related to “Anonymity” and positively related to “Escape.”

CHAPTER 6: IT Security Incidents in Federal Agencies

6.1. Prelude

The previous chapters discuss information theft in the manifestation of insider theft and outsider hacking against four types of organizations. This chapter analyzes IT security incidents beyond information theft in 24 federal agencies. The definitions of information theft, data breach, and IT security incidents are specific in this research, and require some explanation. Information theft can mean a criminal outsider hack, insider theft, or both when plural. Data breaches and IT security incidents alike are any issue where private data is leaked in any form, which can mean an intentional, criminal, unauthorized access, or an accidental, non-criminal leak, such as sending an email to the wrong person. In particular, hacking incidents targeting major federal agencies have become a hot topic in the mass media. For the last few years, confidential information leaked by government employees or contractors have raised doubts about information rights and national security. All of these things considered, there is more need than ever to explore the characteristics of information theft in the federal government.

The Federal Government is a symbol of values cherished in the United States. For example, the Defense Department is a symbol of national security. Some politically motivated hackers abroad as well as internal have tried to penetrate federal IT systems. Beyond obtaining valuable information about the U.S. Government, some hackers may simply want to hack federal systems for reputational purposes. It is assumed that federal IT systems maintain adequate finances, employees, and technologies to keep their data secure.

The Federal Information Security Management Act (FISMA) of 2002 was enacted for the implementation of the information security program, for the evaluation of information security across all federal agencies (GAO, 2011, p. 1). Under this Act, federal agencies must report their IT security incidents to the U.S. Computer Emergency Readiness Team (US-CERT). Because of this act, data regarding information theft in federal agencies is more detailed and well structured than in any other organizations, allowing this research to expand the scope of the incidents being investigated beyond simple characteristics like the date of This chapter discusses the characteristics of IT security incidents not only as intentional criminal offenses, but also cases of human negligence leading to data leaks. IT security incidents by human negligence include IT device theft, dumped or lost documents, information exposure through emails or postal mail, and information exposed by federal services. The goal of this chapter is to identify vulnerable environmental factors that increase the likelihood of IT incidents in federal agencies.

6.2. Overview of IT Security Incidents in Federal Agencies

For this chapter, the term ‘IT security incident’ refers to information theft or the mishandling of assets by fault of employees or contractors. Insider theft rarely goes unreported in the Federal Government, as the available data suggests. Table 27 shows the categories of information theft and data breach.

Table 27: Categories of information theft and data breach

Incident Type	Device/Document	Modus Operandi
Stolen/Lost IT Device	Desktop PC, Laptop PC, Tablet, Smartphone, USB, PC hard drive, Magnetic Tape, other mobile devices	- Stolen from parked car - Burglarized from office - Burglarized from home - Left at public place - Left on public transportation - Disposed of mistakenly - Dumped at trash site - Dumped without deleting protected information - Stolen/ lost with non-encrypted data
Insider Theft	See Chapter 2	See Chapter 2
Hacking	See Chapter 2	See Chapter 2
Dumped/Lost Documents	Documents with protected information.	- Did not shred - Dumped in trash bin without shredding - Dumped in public space - Blown away - Left in public space - Left on public transportation - Forgotten during a move
Internet Exposure	- Protected information on an organization's website - Visible or searchable by web search engines	- Uploaded to organization's website - Uploaded/shared via P2P - Uploaded on a web forum - Information shared by SNS
Exposure of Email/Mail	- Protected information in print. - Protected information attached to an email.	- Sent to wrong address - Sent to a mailing list - Sent unencrypted - Sent with an attached file - Opened during delivery - Seen through envelope window - Missing/lost during delivery

Source: Compiled from OSF & ITRC.

The types of identity theft that federal agencies must defend themselves against are not much different from those that businesses, colleges, and hospitals must watch for. The U.S. Government Accountability Office stresses that confidentiality, integrity, and availability of information should be maintained at federal agencies (GAO, 2011, p.2). As stated earlier in Chapter Two, the number of information thefts reported by the Federal Government to the US-CERT is escalating (GAO, 2014, p.2). However, the GAO report (2012, p.9) indicates that the increase in IT security incidents might be attributed to improved detection systems and the timely reports of incidents from federal agencies, meaning that it may be the ability to detect IT security incidents that has increased, rather than the occurrence of those incidents themselves.

The US-CERT report (2014, p.9) acknowledged that of the 24 major federal agencies, 18 reported inadequate information security controls in 2011. 21 federal agencies identified information security as a major management challenge. The Staff Report on Agency Data Breaches (2006, p.2) concluded that:

(a) data loss is a government wide occurrence,
(b) agencies can be aware of a breach but unaware what was stolen,
(c) only a small portion of data loss was caused by hacking, and
(d) contractors are responsible for many of the reported breaches.

The GAO report (2012, p.2) indicated that, given the vulnerabilities and assessments made in the aforementioned Staff Report on Agency Data Breaches, the negative impact of cyber attacks on government systems include,

> “loss or theft of resources, such as federal payments and collections, inappropriate access to and disclosure, modification, or destruction of sensitive information, disruption of critical operations supporting critical infrastructure, national defense, or emergency services, undermining of agency missions due to incidents that lose the public’s confidence, and use of systems for unauthorized purposes or to launch attacks on other computers systems.”

As national infrastructures have become dependent on data systems and networks, it is noted that the interconnectivity they share make them more susceptible to outside interference (GAO, 2011b, p.2.).

6.3. Research Questions

This chapter identifies environmental factors related to IT security vulnerabilities in The Federal Government. Based on the research questions in Chapter 4, this chapter adds three more research questions guided by Rational Choice theory and Situational Crime prevention perspective.

Research Questions

RQ 1	**Are IT security incidents equally distributed among federal agencies?**
RQ 2	**What kinds of federal agencies are vulnerable to what kinds of IT security incidents?**
RQ 3	**Do IT security incidents show any seasonal variation?**

6.4. Hypotheses

Hackers’ reasons for their criminal activity are most commonly financially, politically, or socially motivated. Occasionally, hacker groups have even claimed they simply wanted to let the IT security community recognize their weaknesses. The kind of organization a hacker targets is dependent on their individual decision-making process. As mentioned, IT security varies from organization to organization based on factors such as management, budget, and organization type. Based on these environmental circumstances, this dissertation proposes the following hypotheses:

Hypotheses

H7	**IT security incidents are more likely to be unequally distributed among federal agencies.**
H8	**Cybercrime-type IT security incidents are more likely to occur at smaller federal agencies.**
H9	**Non-cybercrime type IT security incidents are more likely to occur at larger federal agencies.**
H10	**Non-cybercrime type IT security incidents are not likely to show seasonal variation.**

6.5. Unit of Analysis

In this Chapter, the unit of analysis is the average number of IT security incidents that occurred in 24 federal agencies from 2012-2013. The numbers of IT security incidents in those federal agencies were collected from the reports of Fiscal Year 2012 and the 2013 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002 (Whitehouse, 2012 and 2013). Those IT security incidents were originally reported to the US-CERT. The Presidential Office produced the evaluation reports of those IT security incidents.

6.6. Variables

Federal agencies produce and maintain a vast archive of data and information, produced in digital or paper format and are stored in system servers or secure physical locations. As discussed earlier, these data and information can be hacked, stolen internally, or accidentally leaked by a government employee. These are fairly common problems among governmental organizations. This Chapter examines those failures in IT security, with summarized data released by the Whitehouse and compiled by the US-CERT.

6.6.1. Dependent Variable

IT security incidents in this research are categorized by US-CERT's system. (See Table 28). This research examines the extent of impact from information theft and mishandled data in federal agencies, as well as environmental factors that might be linked to those incidents. Each of the 24 federal agencies researched are given their own incident rates as dependent variables.

Table 28: US-CERT Incident Categories and Definitions

Category/Subcategory	Definition
Unauthorized Access	Unauthorized access is used to categorize all incidents where an unprivileged user gains or may have gained control of a system or resource. Equipment is a specific subset of this category.
Equipment	This subset of unauthorized access is used for all incidents involving lost, stolen, or confiscated equipment, including mobile devices, laptops, backup disks, or removable media.
Denial of Service	This category is used for all successful denial of service attacks, such as a flood of traffic that renders a web server unavailable to legitimate users.
Malicious Code	Used for all successful executions or installations of malicious software that are not immediately quarantined and cleaned by preventative measures such as anti-virus tools.
Improper Usage	Improper usage is used to categorize all incidents where a user violates acceptable computing policies or rules of behavior. These include spillage of information from one classification level to another. Policy violation is a specific subset of this category.
Policy Violation	This subset of improper usage is primarily used to categorize incidents of mishandling data in storage or transit, such as digital personally identifiable information (PII) records or procurement-sensitive information found unsecured or PII being e-mailed without proper encryption.
Social Engineering	Social engineering is used to categorize fraudulent websites and other attempts to entice users to provide sensitive information or download malicious code. Phishing is a subset of social engineering.
Suspicious Network Activity	This category is primarily used for incident reports and notifications created from EINSTEIN and EINSTEIN 2a data analyzed by US-CERT.
Non Cyber	Non Cyber is used for filing all reports of PII spillages or possible mishandling of PII that involve hard copies or printed material rather than digital records.
Other	For the purposes of this report, a separate superset of multiple subcategories has been employed to accommodate several low-frequency types of incident reports, such as unconfirmed third-party notifications, failed brute force attempts, port scans, or reported incidents where the cause is unknown.

Source: The Whitehouse report to Congress (2012)

IT Security Incidents

Table 29 shows the annual average numbers of IT security incidents in the 24 federal agencies. The Veterans Affairs Department recorded the highest average numbers of IT security incidents (9,995). The next highest agency is the Department of Health & Human Services (6,201).

Table 29: Annual average numbers of IT security incidents in 24 federal agencies in 2012-2013.

Department	Average Incidents
Total	52,095
Veteran Affairs	9,995
Health & Human Services	6,201
NASA	5,247
Social Security Administration	4,770
Justice	4,358
Defense	3,712
the Treasury	3,396
Homeland Security	2,632
Transportation	2,578
Commerce	1,879
State	1,469
Agriculture	1,453
Energy	1,092
the Interior	1,034
General Services Administration	445
Housing & Urban Development	434
Education	324
Office of Personnel and Management	238
Environmental Protection Agency	190
US Agency for International Development	188
Labor	178
Nuclear Regulatory Commission	136
Small Business Administration	98
National Science Foundation	48

Source: Compiled from the Whitehouse reports (2012 and 2013).

Total Budget

The total budget at each of the 24 federal agencies sampled is used as an indicator of organization size. It is assumed that federal agencies with the highest budgets will also have the highest amount of human resources and the most powerful IT security systems. Insider theft is considered a human factor for this section of the dissertation. Respective IT management systems are considered environmental factors. Total budgets in these situations are explanatory variables for describing organization sizes. Organizations with more funding are expected to encounter more IT security incidents. The data for total budget outlays at each federal agency were collected from the Fiscal Year 2013 Budget of the U.S. Government (US Office of Management and Budget, 2012). A wide range has been found between the highest and lowest budgets of this list (See Table 30).

Table 30: Total Budgets of 24 Federal Agencies in 2012

Department	Total budget ($/millions)
HHS	889,290
SSA	784,535
DOD	691,471
the Treasury	492,180
Agriculture	140,677
Labor	130,168
Veteran Affairs	122,798
OPM	79,435
Transportation	70,512
HUD	48,528
Education	43,628
Homeland Security	41,648
Justice	29,184
State	26,879
Energy	22,631
NASA	18,432
the Interior	12,279
EPA	8,565
GSA	8,017
NSF	6,910
Commerce	5,704
SBA	5,464
USAID	1,204
NRC	1,053

IT Security Incident Rates as Dependent Variable

IT security incident rates in 24 federal agencies are calculated as follows: First, the average annual numbers of IT security incidents are collected from the above reports. Second, the average annual budgets during 2011, 2012 and 2013 are collected for each agency from the reports of U.S. Office of Management and Budget (2011, 2012 and

2013). Lastly, the IT security incident rates of each agency are calculated by dividing the average IT security incidents per year by the average yearly budget.

6.6.2. Independent Variables

Management, opportunity and incident type factors are categorized with help from the Rational Choice Theory. The ‘management factor’ measures the effectiveness of IT security systems’ management. ‘Opportunity factor’ measures available opportunities to prospective hackers and insiders. ‘Incident type factor’ classifies the methods chosen by hackers and insiders per case. Table 31 shows a brief summary of the dependent and independent variables outlined for this analysis.

Table 31: Description of variables of IT security incidents in federal agencies.

Category		Variables	Description	Data Sources
Dependent Variable	**Incident Rate**	**Incident Rate**	The number of IT security incidents divided by the average amount of budget at each federal agency.	- www.whitehouse.gov. - By calculation
		Average IT Security Incidents	The average number of IT security incidents reported to the U.S.CERT in 2012-2013.	www.whitehouse.gov
		Average Budget	The average amount of annual budget at each federal agency in 2011-2012.	www.budget.gov
Independent Variable	**Management**	**Average Compliance Scores**	Scores of IT security system evaluation directed by the FISMA act.	FISMA act reports in 2011,2012 & 2013 (www.whitehouse.gov)
		IT Security Personnel Rate	The number of IT security employees divided by the total number of employees at each federal agency.	
		IT Security Budget Rate	The amount of IT security budget divided by the total IT budget at each federal agency.	www.whitehouse.gov
	Opportunity	**Number of Employees**	The number of employees at each federal agency.	U.S.OPM
		IT Budget Rate	The amount of IT budget divided by total amount of budget at each federal agency.	- www.whitehouse.gov. - By calculation
		Number of Related Branches	The number of outer sub-organization supervised by the agency.	www.usa.gov
	Incident type	**Cybercrime Type IT Security Incident**	- Denial of service. - Suspicious network activity. - Malicious code. - Unauthorized access. - Social engineering.	www.whitehouse.gov
		Non-Cybercrime IT Security Incidents	- Policy violation. - Equipment. - Non-cyber incidents. - Improper usage.	www.whitehouse.gov
		Unknown Type IT Security Incident	- Others.	www.whitehouse.gov

6.6.2.1. Management variables

Average Compliance Scores

The Federal Information Security Management Act of 2002 (FISMA) requires: “each federal agency to develop, document, and implement an information security program to include a comprehensive risk-based framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets” (E-Government Act of 2002, 2002). FISMA also states that the Inspector General at each federal agency should: “perform periodic assessments of the risk and magnitude of harm, established under the guidelines of the National Institute of Standards and Technology (NIST) that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems” (FISMA Act, 2002). Results from Inspector Generals’ assessments are reported to the Office of Management and Budget, which releases the annual evaluations and compliance scores of the IT security managements. Compliance scores for 2011, 2012, and 2013 were collected from the official ‘Reports to Congress on the Implementation of The Federal Information Security Management Act of 2002’ (Whitehouse, 2011, 2012 and 2013). As exhibited in Figure 7, measured compliance scores for security regulations among the 23 selected agencies vary (OMB, 2012, p. 39). The Social Security Administration shows the highest compliance score, at 97.73. The Nuclear Regulatory Commission and Department of Homeland Security show the second and third highest compliance scores, at 97.13 and 95.98 respectively. The Department of Agriculture shows the lowest score: 29.3. The Department of Health and Human Services and Department of Transportation showed the third and second lowest scores: 52.15 and 47 respectively. The score for the Department of Defense was excluded, as they have been given their own, separate evaluation scoring system. This dissertation hypothesizes that the average compliance scores provided are an important factor in data and information protection for the 23 agencies they belong to.

IT Security Budget Rate

One variable measuring the security of information and data is the IT security budget rate for each agency. This dissertation examines whether or not the budget rate of IT security systems influences their effectiveness or management. The rates of IT security budgets were collected from the same prior cited source, the Report to Congress on the Implementation of The Federal Information Security Management Act of 2002 (Whitehouse, 2012 and 2013).

As stated, the range spending for these budgets was wide (The OMB report, 2012, p.33). The National Science Foundation spent 83.67% of its total budget in IT security during 2012 and 2013. The IT security management budget of the National Science Foundation (NSF) increased dramatically during this period, from 14 million dollars to 151 million dollars. Whether this higher budget will continue in the following years remains to be seen. The Department of Defense spends an average 25.32% of its IT security budget. The Department of Homeland Security spends 15.49%, and the Office of Personnel and Management spends 12.66%. The Department of Agriculture spends only 2.51%, and the Department of Health and Human Services: 2.52%.

6.5.2.2. Opportunity Variables

Number of Employees

As stated, one indicator of any given federal agency’s size is likely the number of employees in that agency. This dissertation hypothesizes that federal agencies with more employees have more IT security incidents than agencies with fewer employees. Because of this hypothesis, number of employees is a variable in analysis. The number of employees as listed in this dissertation are collected from the statistics of the Office of Personnel and Management in 2012.

IT Budget Rate

The total IT budget for each federal agency is a potential indicator of how much data and information are digitalized in those agencies for storage and use. The majority of data and documents are carried and stored in digital formats, which are conveniently searchable and able to be accessed quickly. Despite that convenience, digital data systems are far more vulnerable to massive exposure by outsiders than paper records. Faster processing of information and data also means more difficulty accounting for all of it. The data used to calculate IT budget rates was collected from 2012 and 2013 White House reports.

Numbers of Related Branches for Each Federal Agency

Several federal agencies have sub-organizational agencies which operate under their supervision. This dissertation hypothesizes that government agencies with more sub-organizations will also have more vulnerabilities in their information and data security, as a result of having more systems exchanging information. Access points in more vulnerable sub-organizations may give a way in for hackers and insiders that otherwise would be unable to steal from an agency.

Table 32: Numbers of Related Branches in Federal Agencies

Department	Related Branches
Health & Human Services	17
Agriculture	16
Defense	16
Justice	14
Commerce	13
Homeland Security	10
the Interior	9
Energy	8
Labor	8
Education	7
the Treasury	7
Transportation	7
Housing & Urban Development	6
State	4
Veteran Affairs	3
Environmental Protection Agency	3
Social Security Administration	1
General Services Administration	0
NASA	0
National Science Foundation	0
Nuclear Regulatory Commission	0
Office of Personnel and Management	0
Small Business Administration	0
US Agency for International Development	0

The number of related branches in federal agencies ranged from 17 sub-organizations in the Department of Health & Human Services to 0 sub-organizations in seven other agencies. The source of this data:

http://www.usa.gov/directory/federal/index.html (See Table 32).

6.6.2.3. Incident Type

Cybercrime Type IT Incidents

Cybercrime type IT incidents refer mainly to breaches in IT security caused by hackers operating outside of an agency, but generally cover any situation where IT security is compromised by digital means. The subcategories of cybercrime type IT security incidents are suspicious network activity, unauthorized access, denial of service, malicious code, and social engineering. The data for this variable was collected from the Whitehouse reports (2012 and 2013).

Non-Cybercrime Type IT Security Incidents

Employees, former employees, and contractors of an agency are responsible for the majority of IT security incidents. Not all of these incidents are criminal acts, however, mishandled data and information provide opportunities for hackers across the world. The subcategories of non-cybercrime type IT security incidents are stolen or lost IT equipment, improper usage, policy violation, and non-cyber incidents.

Unknown IT Security Incidents

Unknown IT security incidents are incidents which are, at the time of this dissertation, still under analysis to determine their causes. Some of these incidents could be categorized into the cybercrime type IT security incidents, and others the non-cybercrime type IT security incidents. This category is “employed to accommodate several low-frequency types of incident reports, such as unconfirmed third-party notifications, failed brute force attempts, port scans, or reported incidents where the cause is unknown” (Whitehouse Report, 2014).

Overview by IT Security Incident Types

Among a total of 52,147 IT security incidents averaged from incidents occurring in 2012 and 2013, 28.22% are cybercrime type IT security incidents (14,717 incidents). Non-cybercrime type incidents occupy 64.04% of the total (33,394 incidents). Unknown type incidents are reported at 7.74% (4,036 incidents). These findings are detailed in Table 33 below.

Table 33: Descriptive Statistics of IT Security Incidents at 24 Federal Agencies

Incident type	Subtype	Frequency	Percent
Cybercrime Type Incidents	Malicious Code	8,775	16.82
	Social Engineering	2,994	5.74
	Suspicious Network Activity	2,428	4.65
	Unauthorized Access	490	0.93
	Denial of Service	40	0.08
	Sub total	14,717	28.22
Non-Cybercrime Type Incidents	Non-Cyber	13,965	26.78
	Policy Violation	10,162	19.49
	Equipment	8,441	16.19
	Improper Usage	826	1.58
	Sub total	33,394	64.04
Unknown Type Incidents	Other	4,036	7.74
Total		52,147	

Source: Compiled from the Whitehouse Reports (2012 and 2013).

6.7. Analyses and Results

6.7.1. Descriptive Statistics

Table 34: Descriptive Statistics of Variables in Federal Agencies

Independent variables	N	Mean	Minimum	Maximum	Std. Deviation
Incident Rates	24	5.67	.15	30.15	7.33
Average Incidents	24	2,170.63	48	9,995	2,503.72
Average Budget (in millions of USD)	24	128,483.13	1,053	869,652	2.24
Average Compliance Scores	24	73.61	29	97	17.8
IT Security Budget Rates	24	10.78	2.51	83.67	16.38
IT Budget Rates	24	5.21	.1	24.33	5.73
Employees	24	85,754.33	1,398	758,465	1.61
Related Branches	24	6.21	0	17	5.78
Cybercrime Type Incidents	24	613	39	2,723	780.11
Non-Cybercrime Type Incidents	24	1,391.42	4	8,758	2,081.38

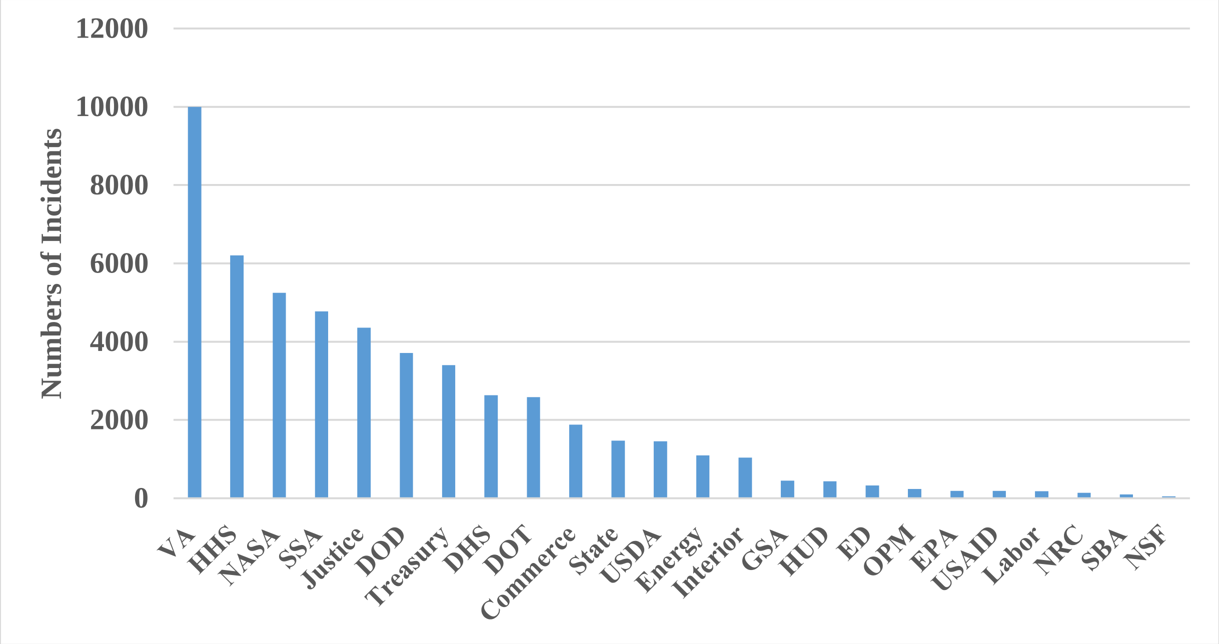
Table 34 shows descriptive statistics for the 10 variables in this chapter of research, with the exception of unknown type IT security incidents.

Hypothesis Tests

H7	**IT security incidents are more likely to be unequally distributed among federal agencies.**

Figure 9 shows the distributions of the averages for IT security incidents during 2012 and 2013 in the 24 federal agencies. Results ranged widely, with the highest average being 8,622 incidents and the lowest being 50. The Department of Veterans Affairs recorded the highest number of IT security incidents for the two year period at 9,995. The Department of Health and Human Services recorded the second highest number of incidents, 6,201. National Science Foundation records the least average of 48 IT security incidents during this period. Federal agency distribution of IT security incidents are not equally presented (χ^2 (23)=66,422.35, p<.01). Five federal agencies, Veterans Affairs, Health & Human Services, NASA, Social Security Administration and Justice Department are the top ranking agencies (20% of total agencies) which records higher numbers of incidents. Total incident numbers from those five agencies are 30,571. Those numbers hold 58.68% of total IT security incidents (52,095) among 24 federal agencies. Unusually, the NASA is a small agency and records a higher number of incidents. It records the highest number of unknown IT security incidents (2,101) among other federal agencies.

Figure 9: Agency Distribution by Average IT Security Incidents in 2012-2013

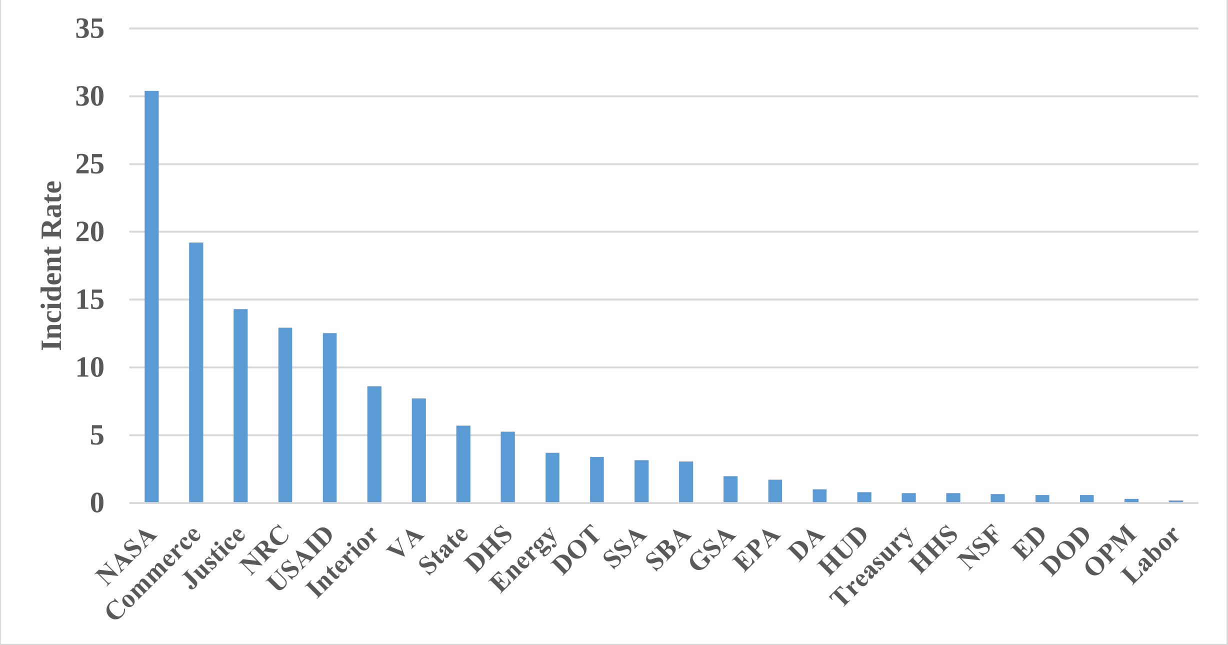


Source: Compiled from the Whitehouse reports (2012 and 2013).

Agency Distribution by IT Security Incident Rate

Figure 10 shows the IT security incident rates in 24 federal agencies. As explained earlier, these rates were calculated by dividing the average number of IT security incidents by the average IT budget at each federal agency. NASA recorded the highest rate, 30.4. The Commerce Department recorded the second highest rate, 19.21. The Department of Defense recorded 0.57 and the Department of Health & Human Services, 0.71. The Office of Personnel Management and Department of Labor recorded the least incident rates, 0.3 and 0.17, respectively. Federal agency distribution of IT security incident rates are not equally presented (χ^2 (21)=180.26, p<.01).

Figure 10: Agency Distribution by IT Security Incident Rate in 2012-2013.

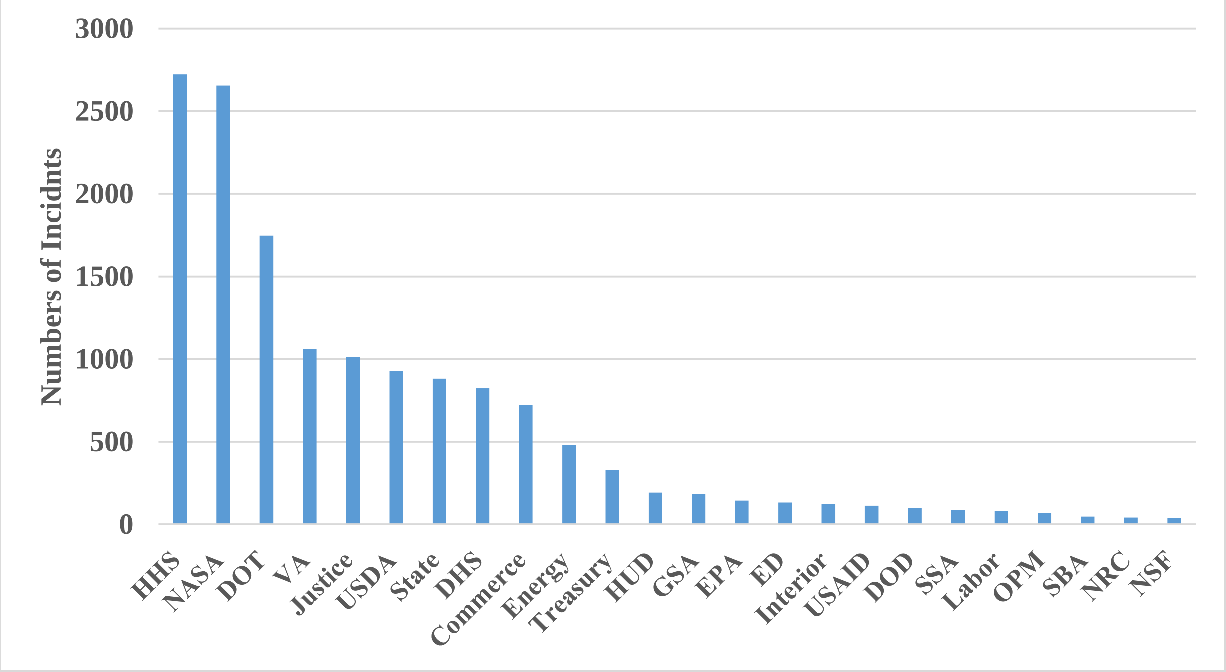


Source: Compiled from the Whitehouse reports (2012 and 2013).

Cybercrime Type IT Security Incidents.

This dissertation ranks the 24 researched federal agencies by frequency of cybercrime type security incidents. The Department of Health and Human Services exhibits the highest frequency of cybercrime (2,723) as compared to other federal agencies. NASA holds the second highest frequency (2,656), and the Department of Transportation holds the third (1,748). These departments are clearly most popular among hackers targeting the Federal Government. Nuclear Regulatory Commission and National Science Foundation record the least numbers of incident, 42 and 39, respectively. These results suggest that the frequency of cybercrime type security incidents in federal agencies is related to their sizes, for each individual agency except the case of NASA. Figure 11 shows the distribution of federal agencies by cybercrime type IT security incidents. Federal agency distribution of cybercrime type of IT security incidents are not equally presented (χ^2 (23)=22,826.29, p<.01). Health & Human Services, NASA, Transportation, Veterans Affairs and Justice Department are the top five agencies (20% of total agencies) which record higher numbers of cybercrime type IT security incidents. Their total numbers are 9,199. These numbers hold 62.5% of total cybercrime type incidents (14,718).

Figure 11: Agency Distribution by Cybercrime Type IT Security Incidents in 2012-2013.



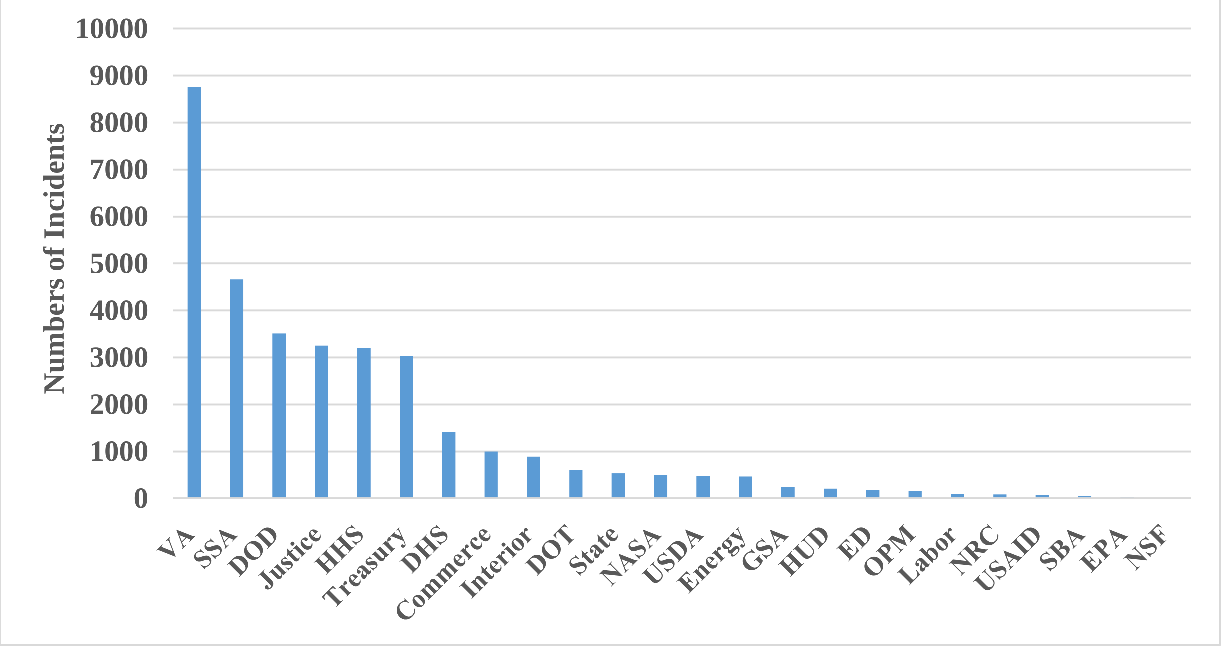
Source: Compiled from the Whitehouse reports (2012 and 2013).

Non-Cybercrime Type IT Security Incidents

Figure 12 shows the distribution of non-cybercrime type incidents among the 24 federal agencies of focus in this research. Federal agency distribution of non-cybercrime type of IT security incidents are not equally presented (χ^2 (23)=71,609.96, p<.01). The Department of Veteran's Affairs records the highest number of non-cybercrime type incidents (8,758) in comparison to other agencies. The Social Security Administration records the second highest number of non-cybercrime type incidents (4,659). The Defense (3,511) and Justice (3,255) departments record the following highest numbers of non-cybercrime type security incident, in that order. Environmental Protection Agency and National Science Foundation record the least numbers of non-cybercrime type IT security incidents, 26 and 4, respectively. These results suggest that the frequency of non-cybercrime type security incidents in federal agencies is related to their sizes, for each individual agency.

Veterans Affairs, Social Security, Defense, Justice, and Health & Human Services are the top five agencies (20% of total agencies) which record higher numbers of non-cybercrime type IT security incidents. Their total numbers are 23,389. These numbers hold 70% of total cybercrime type incidents (33,394).

Figure 12: Agency Distribution of Non-Cybercrime Type Security Incidents in 2012-2013



Source: Compiled from the Whitehouse reports (2012 and 2013).

6.7.2. Bivariate Analyses

The bivariate analysis is performed at this stage to find the relationship between the IT security incident rate and three environmental factors. First, the tests for determining the normality of variable distributions are conducted. Then, the analysis of the bivariate correlations between the IT security incident rate and each independent variable is performed to find their association with each other. Having a small sample size (N= 24) with many variables precluded a multivariate analysis. The 11 variables consisted of normality and non-normality distributions of their data. As a result, the analysis of Spearman's Rho correlations is performed. Table 35 shows the results of this analysis.

Table 35: Correlation Analysis Matrix of IT Security Incidents in 24 Federal Agencies

		Management			**Opportunity**			**Incident Type**		
	Incident Rate	**Compliance Scores**	**IT Security Personnel Rate**	**IT security Budget Rate**	**Employees**	**IT Budget Rate**	**Related Branch**	**Cyber Type Total**	**Non-Cyber Type Total**	**Unknown Type Total**
Incident Rate	1.00									
Compliance. Scores		1.00								
IT Security Personnel Rate		**.475***	1.00							
IT Security Budget Rate		**.756****	**.400+**	1.00						
Employees					1.00					
IT budget Rate	**.827****					1.00				
Related Branch					**.703****		1.00			
Cybercrime Type Incident	**.385+**			**-.451***	**.589****		**.466***	1.00		
Non-Cybercrime Type Incident					**.889****		**.564****	**.571****	1.00	
Unknown Type Incident	**.419***				**.705****	**.401+**	**.540****	**.872****	**.723****	1.00

** p <.01, * p < .05, + p < .1

The IT security incident rate shows a positive relationship with the IT budget rate, cybercrime type incidents, and unknown type incidents. The FISMA compliance scores are found to be of positive relation to the IT security personnel rate and IT security budget rate. This means that those federal agencies which maintain the highest IT security staffing and budget record the highest scores in the IT security management evaluation. The IT security personnel rate shares a positive correlation with the IT security budget rate. The IT security budget rate holds a negative relationship with cybercrime type incidents. Number of employees has a positive relationship with related branches, cybercrime type incidents, non-cybercrime type incidents, and unknown type incidents. The IT budget variable only shares positive relation with unknown type incidents. The related branch variable is positively related to all three types of IT security incidents. Incidents of cybercrime, non-cybercrime, and unknown type all share mutual positive relationships.

Hypothesis Tests

H8	**Cybercrime type IT security incidents are more likely to occur at smaller federal agencies.**
H9	**Non-cybercrime type IT security incidents are more likely to occur at larger federal agencies.**

To test these hypotheses, determinants to measure the size of federal agencies are examined. This research chooses employee numbers and numbers of related branch offices for the determinants of federal agency size. As already discussed in the Part One, it is assumed that a larger organization will create more vulnerabilities and, accordingly, bring more opportunities for offenders. Based on the above data in Table 39, this research examines how a federal agency size influences whether it is more vulnerable to cybercrime type IT security incidents or non-cybercrime type incident. The data characteristics in the examined employees and branch offices are non-parametric. As outlined in the Table 39, the bivariate analyses are performed to determine any statistical difference among the employee numbers, numbers of related branch offices and two types of IT security incidents. The outcomes indicate that the agency size positively related to cybercrime type IT security incidents (r=.589, p<.01) and non-cybercrime type IT security incidents (r=.889, p<.01) as well. The number of related branch offices also is positively related to cybercrime type IT security incidents (r=.466, p<.01) and non-cybercrime type IT security incidents (r=.564, p<.01).

Factor Differences Between the Two Groups

At the next stage, this dissertation divides these 24 federal agencies into two groups according to their IT security incident rates. The significance of differences for these same variables between the 12 federal agencies with the highest incident rates and the remaining 12 with the lowest rates is tested.

Based on normality testing, six variables are found to be normally distributed: average number of incidents, compliance scores, IT security personnel rates, IT budget rates, related branches, and cybercrime type incidents. For those six variables, the significance of the differences between the two groups was tested using the T-test. The remaining five variables: average annual budgets, IT security budget rates, numbers of employees, non-cybercrime type incidents, and unknown type incidents are not normally distributed. For those five variables, the significance of differences between the two groups is tested using the Mann-Whitney *U* Test.

Table 36: Comparison of Two Groups of Federal Agencies by IT Security Incident Rates: Group Rank Means and Significance Test Results†

	Variables	**High Incident Rate Group (Mean)**	**Low Incident Rate Group (Mean)**	**Sig.**
1	Average Incidents	2948.17	1393.08	
2	Average total budget (Millions)	45,985	210,981	
3	Compliance scores	77.17	69.73	
4	IT security personnel rate	1.1	1.96	
5	IT security budget rate	7.87	13.68	
6	Employees	79,263	92,246	
7	IT budget rate	8.62	1.8	*
8	Related branches	5.75	6.67	
9	Cybercrime type incident	812.08	414.33	
10	Non-cybercrime type incident	1,850.67	932.17	+
11	Unknown type incident	287.25	49.08	*

† Variables 1, 3, 4, 7, 8, & 9: T-test.
Variables 2, 5, 6, 10, & 11: Mann-Whitney *U* Test.
$**p<0.01$, $*p<0.05$, $+p<.1$

These analyses indicate that IT budget rate, non-cybercrime type incidents, and unknown type incidents are significantly different between the higher incident rate group and lower incident rate group (See Table 36).

Bivariate Analyses of Environmental Variables and Types of IT Security Incidents

At this stage, this dissertation examines the bivariate relationships between 11 environmental variables and the three types of IT security incidents. For this bivariate analysis, the normality test is performed to determine the normality of distribution for all variables and types of IT security incidents. Results do not satisfy the requirements of the Pearson's Correlation Analysis. Accordingly, the variables and types of incidents are converted to rank order variables in order to perform the Spearman's Rho Correlation Analysis. Table 37 shows the results of the Spearman's Rho Correlation Analysis for environmental variables and types of IT security incidents.

Table 37: Correlation Matrix of Incident Types and Environmental Variables

	Incident Rate	Compliance Scores	IT Security Personnel Rate	IT Security Budget Rate	Employees	IT Budget Rate	Related Branch	Equipment	Policy Violation	Non-Cyber	Improper Usage	Unauthorized Access	Denial of Service	Malicious Code	Suspicious Network	Social engineering	Other
Incident Rate	1.00																
Compliance Scores		1.00															
IT Security Personnel Rate		.46*	1.00														
IT Security Budget Rate		.76**	.4+	1.00													
Employees					1.00												
IT Budget Rate	.77**					1.00											
Related Branch					.7*		1.00										
Equipment					.68*		.52**	1.00									
Policy Violation					.84*		.63**	.68**	1.00								
Non-Cyber					.77**		.51*	.47**	.7**	1.00							
Improper Usage	.49*			.36+	.42*	.72**		.57**	.47*		1.00						
Unauthorized Access					.45*		.48*	.64**	.54**		.46*	1.00					
Denial of Service								.46*			.4+	.7**	1.00				
Malicious Code	.43*				.5*		.42*	.75**	.54**		.58**	.79**	.62**	1.00			
Suspicious Network Activity				-.4+	.67**		.54**	.54**	.62**	.52**		.58**	.44**	.67**	1.00		
Social Engineering	.38+				.44*	.43*	.43*	.57**	.5*		.55**	.73**	.4+	.79**	.6**	1.00	
Other					.71**	.4+	.54**	.72**	.73**	.46*	.57**	.84**	.5*	.83**	.74**	.87**	1.00

** p<.01, * p<.05, +p<.1

Based on the results in Table 37 above, IT security incident rates are positively related to incidents of improper usage, malicious code, and social engineering. Average compliance scores and IT security personnel rate show no relationship with any type of IT security incident. These findings indicate that current IT security evaluations and personnel policy need to be reviewed. IT security budget rates show positive relation to improper usage and negative relation to suspicious network activity. However, these relations are weak ($p<.1$). Agencies' numbers of employees are positively related to all IT security incidents, except incidents of denial of service. These relations indicate that larger federal agencies are more likely to record more IT security incidents. The related branch variable is positively related to most IT security incidents, with the exception of denial of service and improper usage incidents. The results of this bivariate analysis could be grounds for future policy implications meant to reduce IT security incidents in federal agencies. .

6.7.3. Analyses of 'Risky Organizations'

The Risky Facilities Analyses (Eck et al., 2007) operate from the idea that a small number of facilities account for most of the crimes experienced by a group as a whole. This analysis of the concentration of crime is referred to as the 80/20 rule (Clarke and Eck, 2005). It is found that around 80% of crimes occurring at any given set of facilities is caused by a small group (20%) of those facilities. These 20% are called "risky facilities." Most analyses of "risky facilities" are tested with 'established facilities' such as convenience stores, pubs and apartment complexes.

Separately, Clarke and Newman (2006) theorized the concepts of the acronym "EVIL DONE" to outline features that terrorists look for in a target (p.93). They claim that this model is illustrative and shows "how to set about the task of identifying features that make targets vulnerable to attack (p.94)." The elements of the acronym "EVIL DONE" are described as follows (p.94): (1) Exposed - This element indicates that any exposed or visible target that attracts attention is more likely to be attacked. (2) Vital - This element describes that some targets are critical to society's functioning. These targets are referred to as ‘critical infrastructure.’ (3) Iconic - This element applies to any architecture or building that can represent the values or symbols of the United States, such as The Statue of Liberty, World Trade Center, or Pentagon. (4) Legitimate - Public reaction about terrorist actions is critical to continue their terror activities. (5) Destructible - Targets must be able to be significantly damaged if not completely destroyed. (6) Occupied - Terrorists prefer targets that are populated. The best way to spread fear is by killing multiple people. (7) Near - Terrorists tend to choose targets that are easily accessible or close to them, much like common criminals. (8) Easy - Public buildings with little or no security are preferred. Crime-specific “EVIL DONE” model is a useful guidance to develop risk factors to determine what makes hackers prefer some federal agencies as targets over others.

This research uses the term ‘risky organization’ for agencies which are likely to be exposed to IT security incidents. Based on the concepts of “EVIL DONE” and “risky organizations,” this research seeks to identify a group of risky federal agencies: agencies vulnerable to IT security incidents.

The first step in identifying the “risky organizations” is to establish the variables. This research used selected nine variables in two groups, opportunity and vulnerability: rates of IT security incidents, numbers of IT security incidents, total budget, IT security personnel rate, numbers of employees, IT budget rate, numbers of related branch, compliance scores, IT security personnel rate, and IT security budget rate

In the second step, the top five agencies are selected in order from the highest values from the following six variables: rates of IT security incidents, numbers of IT security incidents, total budget, numbers of employees, IT budget rate, numbers of related branch. Those six variables are considered as indicators to provide opportunities for offenders if any agency records higher values at those variables. The rest three variables, compliance scores, IT security personnel rate, IT security budget rate, are indicators for vulnerabilities if lower values are recorded.

In the third step, each of the five chosen agencies in each variable are assigned with scores from the highest, 5 to the lowest, 1. For example, if an agency is ranked at the top in the “A” variable, the agency will get score ‘5.’ For the last above three variables, agencies with the lower values at those variables are assigned scores from 5 to 1 in order.

Fourth, this research adds all ranked scores of agencies assigned from those nine variables. Lastly, the metrics table is made with the ranked agencies assigned scores according to this above scoring methods. Table 38 shows the ranked metrics of each of the top five “risky” federal agencies in nine variables. A total of 17 agencies are listed by these metrics. Of 24 agencies, seven agencies such as Energy, Housing and Urban Development, Office of Personnel Management, Environmental Protection Agency, Education, Labor, National Science Foundation are excluded because those federal agencies are not fallen into any ranks in nine variable categories (See Table 38).

Table 38: Metrics of "Risky organizations" by ranks in each variable.

Rank	Opportunity						Vulnerability		
	Incident Rates	Incidents	Total Budget	Employees	IT budget Rate	Branch	Compliance	IT Personnel Rate	IT security budget Rate
1	NASA	VA	HHS	DOD	Commerce	HHS	USDA	USAID	NASA
2	Commerce	HHS	SSA	VA	GSA	USDA	DOT	USDA	VA
3	Justice	NASA	DOD	DHS	NASA	DOD	HHS	State	HHS
4	NRC	SSA	Treasury	Justice	DHS	Justice	SBA	VA	DOT
5	USAID	Justice	USDA	Treasury	NRC	Commerce	Interior	Interior	SSA

Table 39 shows the total calculations of scores to rank the "risky" agencies. The top seven federal agencies, The Department of Health and Human Services, NASA, Veterans Affairs, Agriculture, Defense, Commerce, and Justice Department are categorized as "risky organizations" in accordance with the above metrics process. The HHS recorded the highest scores, 20, as this department was listed in five "risky" variables. The NASA recorded the second highest scores, 16, and it falls into four variables. The third highest scored agency is Veterans Affairs falling into four variables. The Agriculture Department records the fourth rank with a score of 14 and falls into four variables.

Table 39: Metrics of ranked "Risky organizations" by scores

Variable / Dept.	Opportunity						Vulnerability			Total Scores
	Incident Rates	Incidents	Budget	Employees	IT Budget Rate	Branch	Compliance Scores	IT Personnel Rate	IT Security Budget Rate	
HHS		4	5			5	3		3	20
NASA	5	3			3				5	16
VA		5		4				2	4	15
USDA			1			4	5	4		14
DOD			3	5		3				11
Commerce	4				5	1				10
Justice	3	1		2		2				8
SSA		2	4						1	7
USAID	1							5		6
DOT							4		2	6
DHS				3	2					5
GSA					4					4
Treasury			2	1						3
State								3		3
NRC	2				1					3
SBA							2			2
Interior							1	1		2

6.7.4. Analysis of IT Security System Performance Evaluations

Under Title III of the E-Government Act of 2002 (Public Law, 107-347), the Federal Information Security Management Act (FISMA), "provides a comprehensive framework for supporting the effectiveness of information security controls over information resources that support Federal operations and assets" (Whitehouse, 2014, p.1). FISMA essentially requires federal agencies to minimize risks to information security and potential harm to federal information systems (Whitehouse, 2014). FISMA also gives the Office of Management and Budget (OMB) the responsibility to oversee federal agencies’ information protection activities and submit an annual report on agencies’ information security performance. Finally, the Act requires The National Institute of Standards and Technology (NIST) is required to develop standards and guidelines pertaining to federal information systems (Whitehouse, 2014). As a result of the Federal Financial Reform Act of 1990 (Public Law 101-576), or CFO Act, 24 federal agencies are required to implement FISMA information security protocols. The metrics of those requirements are described in Table 40, below.

Table 40: Summary of FISMA Metrics

No.	Metrics	Summary
1	Information Security Continuous Monitoring (ISCM)	Preventing information security threats by maintaining ongoing awareness of information security, vulnerabilities, and threats to systems and information.
2	Trusted Internet Connections (TIC)	Seeking to optimize and standardize the security of individual external network connections, including connections to the Internet.
3	Strong Authentication: HSPD-12	Implementing policy and formulation of HSPD-12 (identification standard for federal employees and contractors).
4	Portable Device Encryption	Providing the encryption of data at rest and/or in motion to protect data's confidentiality, integrity and/or availability.
5	Domain Name System Security Extensions (DNSSEC) Implementation and Email Validation	Providing cryptographic protections against attacks by digitally 'signing' data. Mitigates the risk of DNS-based attacks and improves the integrity and authenticity of information processed over the Internet.
6	Remote Access	Requiring stronger authentication mechanisms than user ID and password.
7	Controlled Incident Detection	Providing penetration testing to determine whether defenders detect the events (pseudo-incidents) that are discovered during the controlled network penetration test.
8	Security Training	Sponsoring emerging threat exercises to increase cyber security awareness and/or to measure the effectiveness of cyber security awareness training in molding behavior.
9	Automated Detection and Blocking of Unauthorized Software	Implementing an automated capability at the device level to detect and block unauthorized software from initiating.
10	Email Encryption	Implementing of compliant encryption technologies to protect the integrity of the contents and sender information when sending messages to government agencies or the public.

Source: Summarized from the Whitehouse report (2013).

Due to budgetary differences and the characteristics of each department's mission, the levels of IT security systems for the 24 agencies of discussion are assumed to be different. This research hypothesizes that the IT security systems of the 24 federal agencies in question will exhibit varying levels of protection capability against IT security incidents. The metrics of the FISMA capabilities below show the average performance scores of the 24 agencies covered by the CFO ACT for 2010-2013 period (See Appendix IV). In general, the average score of FISMA capabilities have increased from 62% to 81% from 2010-2013. However, total IT security incidents have also increased, from 41,776 to 61,214 during that same period. These findings suggest that IT security detection strength in federal agencies has improved.

Table 41: Correlation Analyses of FISMA Evaluations and IT Security Types at 24 Federal Agencies in 2012-2013

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Monitoring capabilities (1)	1.000																			
Trusted Internet (2)		1.000																		
Authentication (3)			1.000																	
Encrypted IT device (4)	.503*			1.000																
DNSSEC/Email Validation (5)					1.000															
Remote access control (6)				.486*	.459*	1.000														
Controlled incident detection (7)			-.430*				1.000													
Security training (8)								1.000												
Capabilities to detect unauthorized software (9)							.435*		1.000											
Encrypted email (10)										1.000										
Suspicious network activities (11)	-.471*			-.474*		-.502*			-.427*		1.000									
Unauthorized access (12)											.581**	1.000								
DOS (13)											.442*	.696**	1.000							
Malicious code (14)											.672**	.786**	.619**	1.000						
Social engineering (15)				-.448*							.603**	.734**		.786**	1.000					
Equipment Incident (16)										.538**	.536**	.638**	.458*	.749**	.571**	1.000				
Policy Violation (17)						-.478*					.615**	.541**		.542**	.498*	.676**	1.000			
Improper Usage (18)												.456*		.581**	.550**	.568**	.470*	1.000		
Non-cyber incident (19)											.517**					.465*	.700**		1.000	
Other Incidents (20)				-.507*							.743**	.844**	.504*	.833**	.865**	.715**	.727**	.572**	.461*	1.000

** p<.01, *p<.05

Based on available data and the evaluation metrics provided in the Appendix IV, this research performed bivariate correlation analyses between the average evaluation scores of ten FISMA capabilities for 2010-2013 and the average numbers of IT security incidents from 2012-2013 (Appendix II). These bivariate analyses aim at identifying major IT security preparations for detecting and blocking IT security incidents. This research used above ten FISMA categories of Continuous Monitoring Capabilities, Trusted Internet Connections (TIC), Strong Authentication, Portable Device Encryption, Email Validation, Remote Access, Controlled Incident Detection, Security Training, Automated Detection and Blocking of Unauthorized Software, Email Encryption.

The results of the bivariate analyses in Table 41 present several meaningful relationships between variables of FISMA evaluations and IT security incidents. Those relationships are as follows: 1) Monitoring capabilities are negatively related to suspicious network activities. When the monitoring capabilities are timely and actively working, the incidents of suspicious network activities will be decreased, 2) Encrypted portable devices are negatively related to suspicious network activities, social engineering, and other types of incidents, 3) Remote access control is negatively related to suspicious network activities and policy violations. These findings will contribute to establish the policies for IT security incident reduction, 4) Capabilities to detect and block unauthorized software are negatively related to suspicious network activities, 5) Trusted internet capabilities, Email validation policy, and security training are not found any relations with any type of IT security incidents. This research finds that continuous monitoring capabilities are critical factors to detect and block IT security incidents. Further, there are needs to revise and strengthen the overall training programs for IT security staff. On the other hand, the security trainings' effectiveness may not be measurable whether they contribute to detect and block IT security incidents. Overall, suspicious network activities are more found at the current federal IT security policies. More IT security policies should be developed for reducing the non-cybercrime type of incidents.

Chapter Summary

This chapter analyzed IT security incidents beyond information theft in 24 federal agencies. As similar to the previous chapter, different types of federal agencies are assumed to show different types of IT security incidents..

The IT security incident rate shares a positive relationship with the IT budget rate, cybercrime type incidents, and unknown type incidents. The FISMA compliance scores were found positively related to the IT security personnel rate and IT security budget rate. The IT security budget rate shares an inverse relationship with cybercrime type incidents. The number of employees shows a positive relationship with related branches, cybercrime type incidents, non-cybercrime type incidents, and unknown type of incidents. The related branch variable is positively related to all three types of IT security incidents.

From the IT security performance evaluations, under the standards of the NIST, the results of the bivariate analyses present several meaningful relationships between variables of FISMA evaluations and IT security incidents. Monitoring capabilities are negatively related to suspicious network activities. Remote access control is negatively related to suspicious network activities and policy violations. Capabilities to detect and block unauthorized software are negatively related to suspicious network activities. IT security training is found to have limited effectiveness. “Continuous Monitoring” practices exhibit a much higher success rate for the detection of IT security incidents by comparison.

CHAPTER 7:

Non-Cybercrime Type IT Security Incidents at the Department of Veterans Affairs

7.1. Overview of IT Security Incidents

> “On May 3, 2006, a data analyst at Veterans Affairs took home a laptop and an external hard drive containing unencrypted information on 26.5 million veterans, their spouses, and active-duty military personnel. The computer equipment was stolen in a burglary of the analyst's home in Montgomery County, Md., and he immediately reported the theft to both Maryland police and his supervisors at Veterans Affairs. The analyst admitted that he had been routinely taking home such sensitive data for three years. Though the analyst's supervisors knew of the theft, Veterans Affairs Secretary R. James Nicholson was not told of the data theft until May 16.” (http://epic.org/privacy/vatheft/)

The aforementioned incident is well known to the IT security community as one of the largest IT security failures in the U.S. This type of incident can occur at any organization. This chapter presents more in-depth research about IT security incidents reported by the Department of Veterans Affairs. For the last few years, Veterans Affairs has experienced problems with IT security frequently (See Table 42). Across all federal departments, Veterans Affairs suffers the most IT security incidents, accounting for 19.9% of the total incidents in the entire federal governments.

Table 42: VA’s IT Security Incidents Reported to the US-CERT in 2007-2013.

Year	Total	2013	2012	2011	2010	2009	2008	2007
No. of Incidents	51,148	11,382	8,618	6,586	7,513	6,843	5,372	4,834

Source: VA report to Congress (May 25, 2014).

Under Public Law 109-461 (Dec 2006), the Department of Veterans Affairs is required to report its monthly and quarterly data breaches to Congress. Reports by independent auditors hired by Veterans Affairs reveal that the department exhibited continuous control weaknesses in its IT security control system from 2007-2013 (See Table 43).

Table 43: IT Security Control Weaknesses in the VA Department

Security Control Category	2007	2008	2009	2010	2011	2012	2013
Access Control	✓	✓	✓	✓	✓	✓	✓
Configuration Management	✓	✓	✓	✓	✓	✓	✓
Segregation of Duties	✓	✓	✓	✓	✓	✓	✓
Contingency Planning	✓	✓	✓	✓	✓	✓	✓
Security Management	✓	✓	✓	✓	✓	✓	✓

Source: Compiled from the GAO report (Mar 25, 2014).

Data pertaining to IT security incidents at the Department of Veterans Affairs has been obtained via their reports to Congress from 2011 to 2014. Monthly reports from this period detailed non-cybercrime type IT security incidents. Table 44 displays all available data regarding non-cybercrime type IT security incidents at the Department of Veterans Affairs.

Table 44: Non-Cybercrime Type IT Security Incidents at the VA Department in 2011-2014

	Total	IUEEI[1]	MHIts[2]	MMI[3]	CMOPI[4]	Equip. inventory[5]	PC[6]	Laptop[7]	Mobile Devices[8]
Total	16,841	4,281	5,057	5,458	276	157	116	365	1,131
2014	4,602	1,089	1,313	1,710	49	37	15	41	348
2013	4,171	974	1,345	1,350	68	45	27	103	259
2012	4,382	1,234	1,365	1,304	56	35	39	97	251
2011	3,687	984	1,034	1,094	103	40	35	124	273

1. Internal Un-encrypted Email incidents, 2. Mishandled Incidents, 3. ‘Mis-mailed’ incidents, 4.Mis-mailed CMOP incidents, 5. IT Equipment Inventory Incidents, 6. Missing/Stolen PC incidents, 7. Missing/stolen laptop incidents, 8. Lost mobile devices.

The IT security incident subcategories outlined in Table 52 include mismanagement and employee mistakes. During a four year period, the most common non-cybercrime type IT security incident at the Department of Veterans Affairs was ‘mis-mailing’, accounting for 5,458, or 32.4% of the total incidents at the department for that period. The second most common non-cybercrime incident was mishandling, accounting for 5,057, or 30% of those incidents. The third most common problem of these subcategories was internal unencrypted email, at 4,281 or 25.4% of total non-cybercrime IT incidents. Considering that the Department of Veterans affairs has three related branches and is responsible for 234 medical centers nationally, it is little surprise that they encounter so many inside mishandlings of data and information.

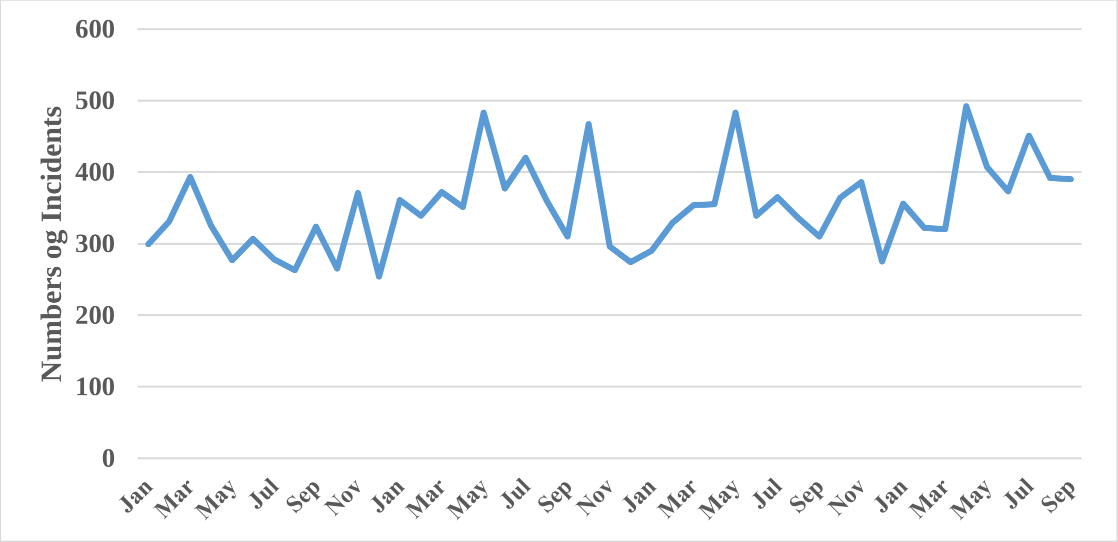
The following sections discuss the seasonal variations of non-cybercrime type IT security incidents. This dissertation categorizes these incidents into two subtypes. The first subtype being mis-handled data and information. This subtype includes internal unencrypted email incidents, mishandling incidents, mis-mailing incidents, and mis-mailed CMOP (Consolidated Mail Outpatient Pharmacy) incidents.

The second subtype is mis-handled equipment, and includes IT equipment inventory incidents, missing/stolen PC incidents, missing/stolen laptop incidents, and lost mobile devices. Incidents falling under this second subtype can occur because of employee negligence or theft by outside offenders.

7.2. Seasonal Variations of Non-Cybercrime Type IT Security Incidents at the VA Department

Figure 13 demonstrates the seasonal variations of the total non-cybercrime type IT security incidents in the Department of Veterans Affairs from 2011- 2014. It indicates that total non-cybercrime type IT security incidents were reported more frequent during late spring (April-May) for the duration of the sample period.

Figure 13: Seasonal Variations of Non-Cybercrime Type IT Security Incidents at the VA Department in 2011-2014

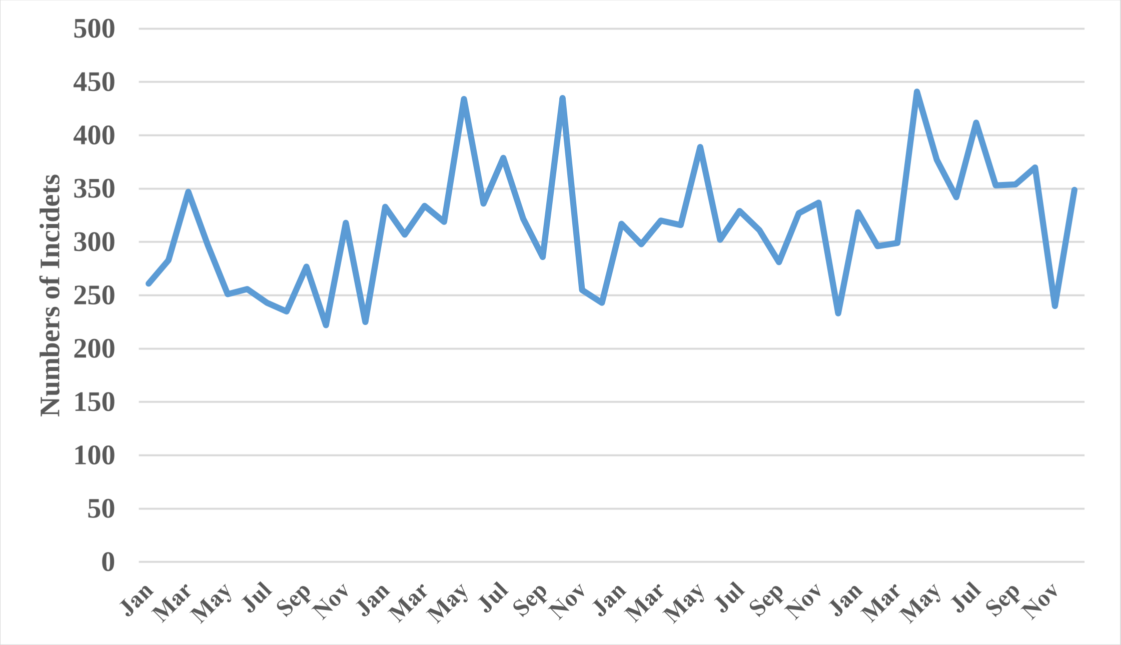


Source: Compiled from the VA monthly reports during 2011-2014.

7.3. Seasonal Variation in Incidents of Mis-handled Information at the VA Department

Figure 14 displays incidents of mis-handled information, (which fall under the first subtype of non-cybercrime type IT security incidents) for the Department of Veterans Affairs, from 2011 to 2014. Instances of mis-handled information are presumed to not show seasonal variation. This presumption comes from the plain reality that employees capable of mis-handling information are working with that data on a daily basis each year, so accidents should be no more likely at one time versus another.

Figure 14: Seasonal Variations in Mis-handled Information at the VA Department in 2011-2014

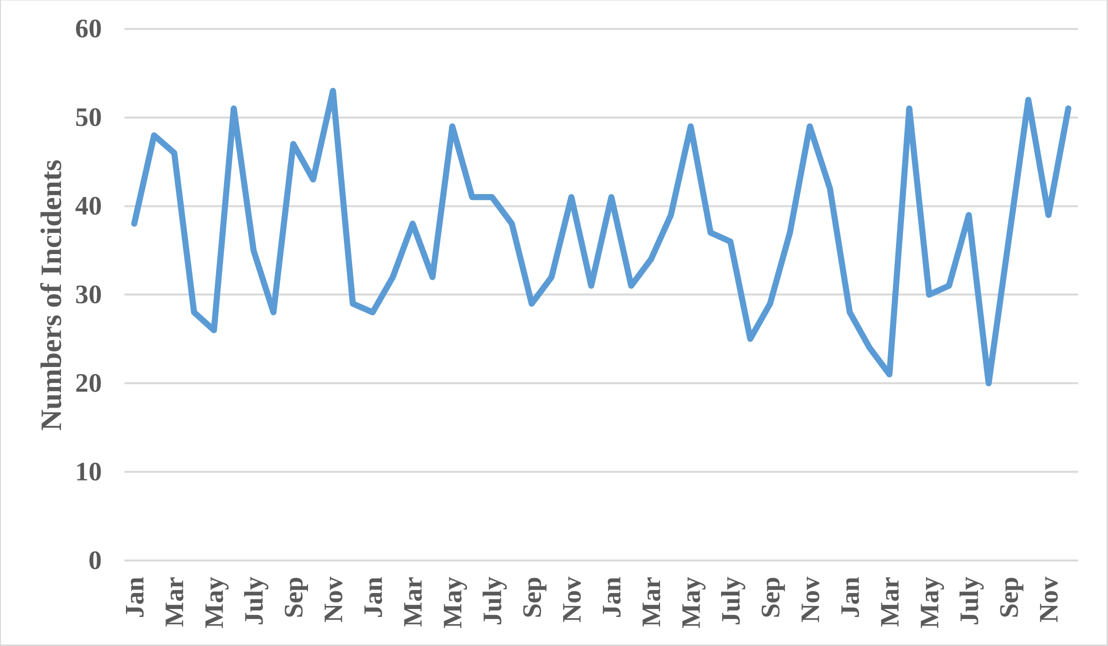


Source: Compiled from the VA monthly reports during 2011-2014.

7.4. Seasonal Variation in Incidents of Stolen/Missing IT Devices at the VA Department

Figure 15 displays the incidents of stolen/missing IT devices at the Department of Veterans Affairs during the 2011-2014 period. This subtype, missing equipment, includes IT equipment inventory incidents, missing/stolen PC incidents, missing/stolen laptop incidents, and lost mobile devices. 'IT devices' refers to anything from a personal computer, to a laptop, to a cellphone issued to employees by the department. All of these devices are presumed to include sensitive data and information related to the department's operations. Instances of stolen/missing IT devices are presumed to show seasonal variation. This presumption comes from the current research about property offenses which showed time patterns.

Figure 15: Incidents of Stolen/Missing IT Devices at the VA Deparment in 2011-2014



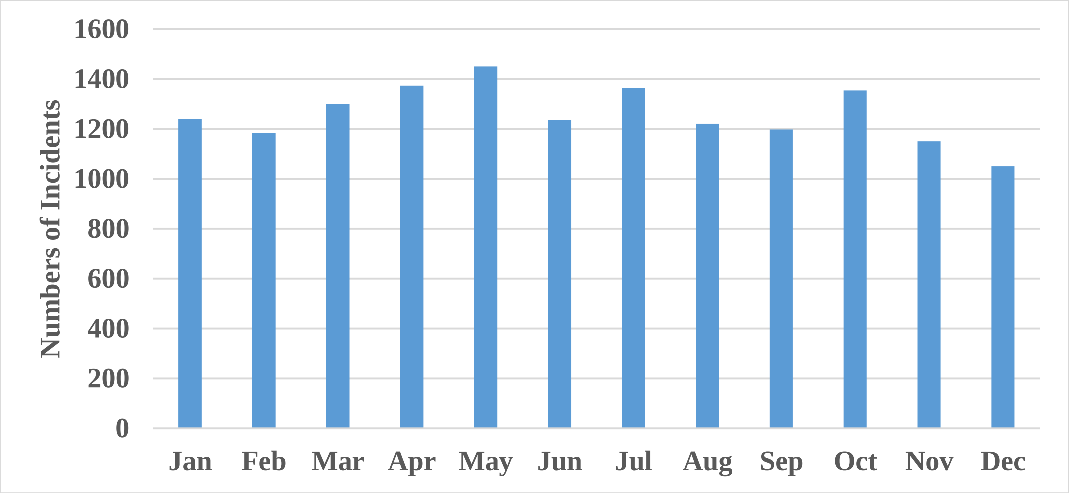
Source: Compiled from the VA monthly reports during 2011-2014.

Hypothesis Tests	
H10	**Non-cybercrime type IT security incidents are not likely to show seasonal variation.**

Seasonal variation of mis-handled information

For exploring the monthly differences, this research counted all incident numbers by month during these four years from the Department of Veterans Affairs. Incidents of mis-handled information including mis-mailing incidents are reported most frequently around May and least reported in December (See Figure 16). The Chi-square test of equality of month support this finding (χ^2 (11) = 110.049, p <.01). This seasonal variation of mis-handled information suggests a proper policy implication to reduce those incidents.

Figure 16: Seasonal variation of Mis-handled Information at the VA Department in 2011-2014.

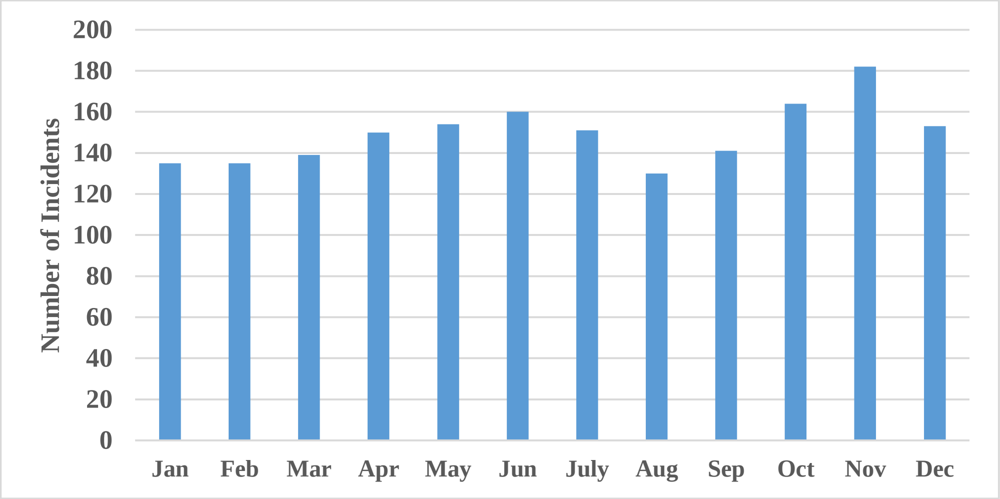


Source: Compiled from the VA monthly reports during 2011-2014.

Seasonal variation of Stolen/Missing IT Devices

This subcategory means that this pattern could be one of several things, such as employees simply losing their government-issued laptops, or increased burglaries of offices and facilities belonging to the branch offices of Veterans Affairs. Around the months of June, October and November for the recorded four year period, incidents of stolen/missing IT devices show an increasing pattern in comparison to other months (See Figure 17). However, the Chi-square test of equality by month does not support this seasonal variations (χ^2 (11) = 16.02, $p=.14 > .05$). There will be a need to watch over these incidents in more extended period of time. This finding also suggests a proper policy implication to reduce those incidents.

Figure 17: Seasonal Variation of Stolen/Missing IT Devices at the VA Department in 2011-2014.



Source: Compiled from the VA monthly reports during 2011-2014.

Chapter Summary

This chapter describes non-cybercrime type IT security incidents reported by the Department of Veterans Affairs from 2011-2014. The VA reports to Congress that IT security incidents at the VA Department had increased from 2007-2014. The VA Department is required by law to report its IT security incidents to Congress on a monthly basis. Total non-cybercrime type IT security incidents are reported as increasing from 2011-2014. Incidents of mis-handled data and information show statistical seasonal variations. However, incidents of stolen/missing IT devices does not show statistical seasonal variation. Reflection on these findings will reduce IT security incidents at the VA Department.

Chapter 8: Conclusions

8.1. Summary of Findings.

Testing the hypotheses for a relationship between organization size and information theft type revealed that insider thefts are more common than hacking where larger businesses are concerned. Despite being so common, insider theft also has a longer detection time than hacking at larger businesses. In education, hacking is exceedingly more common than insider theft at large colleges and universities. Insider thefts take longer to detect in education, as is to be expected from their rarity in this situation. In large hospitals and medical centers, insider theft is more common than hacking. Just as in businesses and schools, insider theft in hospitals take longer to detect than hacking. In government, hacking and insider theft alike are more common at the state level, in comparison to federal, local and city governments. As in every other organization, insider theft in government takes longer to detect than hacking.

Businesses show no seasonal variation for hacking attacks. However, schools and universities show seasonal variation for hacking. Due to a lack of relevant data, hackings that target healthcare facilities were not analyzed for seasonal variations in this research. Insider theft was not analyzed for seasonal variations since insider thefts are presumed to be equally probably any time of the year in which employees or contractors are working.

The SCAREM model test was performed for recorded hacking incidents. Hacking incident rates have been found positively related to the concept of ‘Reconnaissance’ (The ‘R’ in ‘SCAREM’). This means that higher hacking rates in any given organization correspond with a longer detection time for hacking incidents in that organization. The SCAREM model was also tested for insider theft. Insider theft rates have been identified as positively related to the concept ‘Escape.’ This means that organizations which experience more insider theft will also take longer to detect instances of insider theft.

For the analysis of information theft in federal agencies, data was divided into eight categories: unauthorized access, equipment lost/stolen, denial of service, malicious code, improper usage, policy violation, social engineering, suspicious network activity, non-cyber type incident, and other incidents. IT security incident rates were measured by dividing the average number of incidents during the 2012-2013 period by the total budget at each federal agency. Among the 24 agencies for which this rate was measured, NASA recorded the highest. The Department of Commerce and Department of Justice showed the next highest rates of IT security incidents. In the bivariate analysis testing for relationships between IT security incident rates, management factors, opportunity, and incident types, IT security incident rates were found positively related to IT budget rate, cyber-crime type incidents, and unknown type incidents. In the analysis of factor differences between the higher IT security incident rate group and lower IT security incident rate group, the IT budget rate, non-cybercrime type, and unknown type incidents also showed significant differences.

Based on a framework of “Risky organizations,” this research created a metrics used nine variables to determine opportunities and vulnerabilities for IT security incidents. With these metrics, the Department of Health and Human Services, NASA, Veterans Affairs, Agriculture, Defense, Commerce, and Justice Department are found to be the most vulnerable targets for hackers.

This research used data from the Department of Veterans Affairs to measure the seasonal variation of non-cybercrime type IT security incidents. Data from 2011-2014 revealed that these types of incidents indeed have seasonal variation.

8.2. Research Limitations

Certain limitations prevent this research from establishing a comprehensive overview of information theft across all four classes of organizations. There is no national database recording all instances of information or identity theft. The Federal Trade Commission and FBI handle reports from victims of cybercrime, and those two agencies only release incident summaries annually. The US-CERT does not release detailed data regarding IT security incidents in federal agencies. Due to the shortcomings of these sources, this research uses information theft data provided by two non-profit organizations: the ITRC and OSF. Those two organizations amassed their data mainly from media sources and several State Attorneys' Offices. The lists compiled by these organizations do not provide an in depth review of information thefts, and mass media are not the most reliable source. Consequently, many small scale information thefts are likely unreported. In addition, businesses tend to keep information thefts private to protect their prospective sales, market shares, and reputation. Actual incidents of data breach, identity theft, and general cybercrime are assumed under-reported. In many cases, victims of information theft are not aware a crime has been committed against them.

There are very few studies exploring the actual quantity of data breaches in the U.S., or how many of those breaches result in fraud. Due to the lack of such studies, this research did not have sufficient information for examining the relationship between data breaches and follow up crimes such as fraud. There are also very few studies on information theft in educational and medical organizations in comparison to business and government organizations. As new data and information are produced every day, the opportunities for their exploitation increase simultaneously. The occurrence of information theft exceeds its being tracked to such an extent that the damages they cause are immeasurable. For more detailed analysis of these incidents, launching an academic level database for data and information theft is recommended.

Though incapable of creating one, this research proposes a model for an academic database of data and information theft. The elements of the theoretical database are based on four functions: 1) identifying the incident, 2) collecting information about the incident, 3) analyzing the incident, and 4) releasing analysis of the incident to the public. Specific actions for each step are described in Table 54.

Table 45: ICAR (Identify, Collect, Analyze, and Release) Research Model Description.

Stage	Identification	Collection	Analysis	Release
Actions	- Receiving direct reports from citizens - Collecting incident cases from mass media - Sharing information with other organizations	- Contacting other research organizations - Conducting more research - Collecting information of incidents based on Freedom of Information Act in concerned states - Receiving feedback from victim organizations	- Analyzing the data - Conducting a follow-up study - Conducting a victim survey	- Publishing an analysis report - Planning a public awareness campaign - Operating a website

According to FTC report, California, Texas, and Florida, are top three states which are reporting the most frequent ID theft cases. This research is focused on a national scale of information incidents over affected organizations across the states. The next step of information theft research is recommended for a state level studying in more in-depth analysis with a support of a state attorney office where receives the data breach incidents with more than 500 affected victims per an incident.

8.3. Policy Implications

This research suggests policy implications for managing data and information across all types of organizations by identifying which types are most vulnerable to information theft. The conclusion is that information theft may occur at any type of organization. Outside hackers often possess skills superior to those of the IT security staff at the organizations they hack. Worse still, inside employees of organizations are able to steal data and information at any time. The most vital security measure in guarding against information theft from hackers and insiders alike is constant monitoring of all valuable data and information. In-house training for IT security system management and enhancement of the ethics of information and data handling are also recommended for information theft prevention and detection.

In accordance with the data used in this research, the Situational Crime Prevention model was adapted to generate methods of opportunity reduction in information theft prevention. Focusing on environmental factors, this model of e-commerce developed 25 specific techniques applying to information theft (see Appendix VIII).

Some prevention methods suggested in this research may overlap with other techniques. Some methods may seem vague, or too costly. Regardless of personal opinions, the analyses conducted in this research all point to a need for constant monitoring of data and information: the most crucial measure in information theft prevention.

8.4. Final Remarks

Organizations of all types collect a variety of data and information from their customers or constituents. With this data, those organizations can produce new information. Web applications, mobile devices, point-of-sale devices, and medical devices are just a few of the objects allowing customers and constituents to access organizations' data. Information technology itself has produced a wide array of convenient tools for the rapid viewing and sharing of data. Unfortunately this comes with the negative consequence of additional vulnerabilities in IT management systems.

This dissertation developed research questions and hypotheses related to situational factors surrounding organizations experiencing information theft. Organizational size and type were two such situational factors found to be of critical importance. This research examined issues in the contemporary study information theft, and expanded the term 'information theft' to include data breach and identity theft.

Data used in this research has its own internal limitations. First, the data is not 'official': it was not compiled by law enforcement or any other government agency. Second, public media resources cannot, at their present state, record every instance of information theft across the nation, especially as they seem to focus on larger, more sensational IT security incidents that attract public attention. Third, the response rates for past surveys on data breach and identity theft are very low. Finally, very few academic studies have been conducted with attention to IT security incidents at educational and medical organizations. In light of these four limitations, public media sources are the most viable for information theft at present.

This research used Rational Choice Theory to dissect the decision making processes of information theft perpetrators. This approach is suitable in that information thieves are neither violent nor impulsive, and therefore take great care before their crime. To commit an information theft, criminals need at least a minimal level of knowledge regarding information technology and technical training. Outside hackers and insiders tend to spend a certain amount of time preparing for their crimes, and they consider the surrounding environmental factors that may produce vulnerabilities in their target IT systems. They calculate the potential rewards and risks for committing to a hacking or insider theft before initiating it.

For information theft prevention, this research applied the Situational Crime Prevention Theory. Information theft may garner public attention in comparison to violent crime, yet organizations are often defenseless against information theft when targeted by hackers with advanced technology. Most people are unaware of this and the other dangers of unchecked information theft. This research suggests that a comprehensive diagnosis of IT management systems’ vulnerabilities may reduce the damages of information theft in any organization type.

This research proposes that a comprehensive database be launched to collect and analyze information theft in greater detail. Some organizations, particularly businesses, tend not to disclose IT security incidents in fear of losing the confidence of their clients or constituents. There are presently some laws regarding the handling of identity theft and data breach, which have been found to contribute to a decline in data breach when legislated at the state level.

The effects of individual and organizational awareness training provide limited protection against information theft. Regular, comprehensive analyses for vulnerabilities in IT security systems is likely the only effective way to curb information theft, whether those thefts be attempted from inside or out of an organization. Constant IT monitoring is at present the only guaranteed method for information theft prevention and detection at the organizational level.

Limitations in available data prevented a study of the circulation mechanism for stolen data and information. Future research will explore how stolen data and information are disposed of and traded in underground markets by individual and group criminals.

Chapter Summary

This chapter summarizes the findings made by this research. Research limitations and possible policy implications are addressed as well. There is no national level database to record and analyze data breaches and identity thefts. The limitations of data used here are also presented. For a more in-depth analysis of information theft, this research develops its own model, ‘ICAR’ (Identification, Collection, Analysis and Release) as a suggestion. This model describes the methods of collecting and analyzing data regarding information theft incidents.

This chapter suggests possible methods of information theft prevention. Many organizations do not consider information theft a serious threat, thus why it is so damaging. In-house training sessions for employees may help protect data and information, but comprehensive, constant analyses for vulnerabilities in IT management systems prove more effective, and are recommended. Few organizations' IT networks are without vulnerabilities; the more vulnerabilities that go unchecked, the more opportunities there are for insiders and hackers to exploit them. Because of this, constant, routine monitoring of IT management systems is necessary. This research presents a few potential models of information theft prevention based on Situational Crime Prevention Theory.

References

Achtzener, D. (2009). *Data breaches within the federal government*. Fairfax, VA: George Mason University. Retrieved from http://s3.amazonaws.com/chssweb/documents/1041/original/Achtzener_final.pdf?1304690801.

Acquisti, A., Friedman, A., and Telang, R. (2006). *Is there a cost to privacy breaches? An Event research*. Presented at 27th International Conference on Information Systems, Milwaukee. Retrieved from http://www.heinz.cmu.edu/~acquisti/ papers/acquisti-friedman-telang- privacy-breaches.pdf.

Allison, S., Schuck, A., and Lersch, K. M. (2005). Exploring the crime of identity theft: prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice, 33,* 19-29.

American Hospital Association. (2010). *Statement of the American Hospital Association to the Senate Commerce, Science and Technology Committee: Consumer Protection, Product safety, and Insurance Subcommittee. The data security and breach notification act of 2010*. Chicago, IL: Author. Retrieved from http://www.aha.org/advocacy-issues/testimony/2010/100922-tes-breachnotif.pdf.

American Health Association. (2012). *2012 AHA Guide*. Chicago, IL: Author.

Application Security, Inc. (2010). An examination of database breaches at higher education institutions. Retrieved from http://www.appsecinc.com/techdocs/whitepapers/Higher-Ed-Whitepaper-Edited.pdf.

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology, 4*(1&2), 643-656.

Baum, K. (2006). *Identity theft, 2004*. Washington, D.C.: Bureau of Justice Statistics. Retrieved from http://bjs.ojp.usdoj.gov/content/pub/pdf/it04.pdf.

Baum, K. (2007). *Identity theft, 2005*. Washington, D.C.: Bureau of Justice Statistics. Retrieved from http://bjs.ojp.usdoj.gov/content/pub/pdf/it05.pdf.

Baum, K. and Langton, L. (2010). *Identity theft reported by households, 2007-Statistical tables*. Washington, D.C.: Bureau of Justice Statistics. Retrieved from http://bjs.ojp.usdoj.gov/content/pub/pdf/itrh07st.pdf.

Becker, G. (1968). Crime and punishment: An economic approach. *The Journal of Political Economy*, *76*, 169-217.

Burd, S. (2008). *Impact of information security in academic institutions on public safety and security in the United States, 2005-2006*. doi:10.3886/ICPSR21188.v1.

Campbell, K., Gordon, L., Loeb, M., 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.

Cappelli, D.M., Moore, A.P., Shimeall, T.J., and Trzeciak, R.J. (2006). *Common Sense guide to prevention and detection of insider threats: Version 2.1*. Pittsburgh, PA: Carnegie Mellon University. Retrieved from http://www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.1-1-070118.pdf.

Cappelli, D., Moore, A., Trzeciak, R., and Shimeall, T.J. (2009). *Common sense guide to prevention and detection of insider threats. 3rd Edition-Version 3.1*. Pittsburgh, PA: CERT/Carnegie Mellon University. Retrieved from www.cert.org/archive/pdf/CSG-V3.pdf.

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 Journal of Electronic Commerce*, *9*(1), 70-104.

Clarke, R.V. (1980). Situational crime prevention: Theory and practice. *British Journal ofCriminology*, *20*(2), 136-147.

Clarke, R.V. (1983). Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice*, *4*, 225-256.

Clarke, R.V. (1995). Situational crime prevention. In M. Tonry & D. Farrington (Eds.). *Crime and justice: A review of research* (p. 91-150). Chicago, IL: University of Chicago Press.

Clarke, R.V. (1997). Situational crime prevention: Successful case studies (2nd ed.). Guilderland, NY: Harrow and Heston.

Clarke, R.V. (2008). Situational Crime Prevention. In R. Wortley and L. Mazerolle. (Eds.), *Environmental Criminology and Crime Analysis* (pp. 178-194). Oregon: Willan Publishing.

Clarke, R.V. and Cornish, D.B. (2001). Rational Choice. In R. Paternoster and R. Bachman, R. (eds.), *Explaining Criminals and Crime: Essays in Contemporary Theory.* Los Angeles, CA: Roxbury.

Clarke, R.V. and Newman, G. R. (2006). *Outsmarting the terrorists*. Westport, CT: Praeger Security International.

Clarke, R.V. and Eck, J. E. (2007). Crime analysis for problem solvers in 60 small steps. Washington, D.C.: Office of Community Oriented Policing Services, Department of Justice. Retrieved from http://www.popcenter.org/Library/RecommendedReadings/60Steps.pdf.

Copes, H. and Vieraitis, L. (2009). Bounded rationality of identity thieves: Using offender based research to inform policy. *Criminology and Public Policy, 8*(2), 237-262.

Cornish, D.B. and Clarke, R.V. (1986). *Reasoning criminal: Rational choice perspectives on offending.* New York, NY: Springer-Verlag.

Cornish, D.B. and Clarke, R.V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, *25*(4), 901-916.

Cornish, D.B. and Clarke, R.V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, *16*, 41-96.

Cornish, D.B. and Clarke, R.V. (2008). The Rational Choice Perspective. In R. Wortley and L. Mazerolle. (Eds.), *Environmental Criminology and Crime Analysis* (pp. 21-47). Oregon: Willan Publishing.

Computer Security Institute. (2010). *2010 CSI Computer Crime and Security Survey*. New York: Author. Retrieved from https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf.

Copes, H., Kerley, K.R., Huff, R., and Kane, J. (2010). Differentiating identity theft: An exploratory research of victims using a national victimization survey. *Journal of Criminal Justice, 38*, 1045-1052.

Copes, H. and Vieraitis, L.M. (2009a). Bounded rationality of identity thieves: Using offender-based research to inform policy. *Criminology & Public Policy*, *8*(2), 237-262.

Copes, H. and Vieraitis, L. (2009b). Understanding identity theft: Offenders' accounts of their lives and crimes. *Criminal Justice Review*, *34*, 329-349.

CSO Magazine, Software Engineering Institute, Deloitte, & U.S. Secret Service. (2011). *2010Cybersecurity watch survey: Cybercrime increasing faster than some company defenses*. Retrieved from http://www.cert.org/archive/pdf/ecrimesummary10.pdf.

Cummings, A., Lewellen, T., McIntire, D., Moore, A.P., and Trzeciak, R. (2012). *Insiderthreat research: Illicit cyber activity involving fraud in the U.S. Financial services sector*. Pittsburgh, PA: CERT/Carnegie Mellon University. Retrieved from http://www.sei.cmu.edu/reports/12sr004.pdf.

Danchev, D. (2008, October 29). *CardCops: Stolen credit card details getting cheaper*. Retrieved from http://www.zdnet.com/blog/security/cardcops-stolen-credit-card-details-getting-cheaper/2084.

D'Arcy, J., Hovav, A., and Galletta, D. (2008). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 1-20. doi 10.1287/isre.1070.0160.

Davis, T. and Waxman, H. A. (2006). *Staff report: Agency data breaches since January 1,2003*. Washington, D.C.: Government Reform Committee. Retrieved from http://www.wired.com/images_blogs/ threatlevel/files /AgencyBreachSummary Final.pdf.

Denning, D. (1999). *Information Warfare and Security*. Boston: Addison-Wesley.

Dixon, P. (2006). *Medical identity theft: The information crime that can kill you*. World Privacy Forum. Retrieved from http://www.worldprivacyforum.org/pdf/wpf_exsum_medidtheft2006.pdf.

Federal Trade Commission. (2009). *Consumer sentinel network data book 2008*. Washington, DC: Author. Retrieved from http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf.

Felson, M. and Clarke, R. V. (1998). *Opportunity makes the thief. Practical theory for crime prevention*. Police Research Series, Paper 98. Policing and Reducing Crime Unit, Research, Development and Statistics Directorate. London, U.K.: Home Office. Retrieved from www.homeoffice.gov.uk/rds/prgpdfs/fprs98.pdf.

Finklea, K.M. and Theohary, C.A. (2013). *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. Washington, DC: Congressional Research Service. Retrieved From http://www.fas.org/sgp/rs/misc42547.pdf.

Foley, L. (2003). *Identity theft: The aftermath 2003*. San Diego, CA: The Identity Theft Center. Retrieved from http://www.idtheftcenter.org/idaftermath.pdf.

Floridi, L. (2005). Is semantic information meaningful data? *Philosophy and Phenomenological Research*, *70*(2). 351-370.

Gaynor, M.S., Hydari, M.Z., and Telang, R. (2012). *Is patient data better protected in competitive healthcare markets?* Presented at workshop on economics of information security (WEIS 2012).
Retrieved from weis2012.econinfosec.org/papers/Gaynor_WEIS2012.pdf.

Gerard, G. J., Hillison,W., and Pacini, C. (2004). Identity theft: The US legal environment and organizations' related responsibilities. *Journal of Financial Crime*, *12*, 33-43.

Gordon, G. R., Rebovich, D., Choo, K., and Gordon, J. B. (2007). Identity fraud trends and patterns: Building a data-based foundation for proactive enforcement. Utica, NY: Center for Identity Management and Information Protection. Retrieved from http://www.utica.edu/academic/institutes/cimip/publications /index.cfm.

Graboski, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies,10(2)*, 243-249.

Greene, M.N. (2009). Divided we fall: Fighting payments fraud together. *Federal Reserve Bank of Chicago Economic Perspectives*, 1st Quarter, 37-42.

Hanley, M., Dean, T., Schroeder, W., Houy, M., Trzeciak, R.F., and Montelibano, J. (2011). *An analysis of technical observations in insider theft of intellectuall property cases*. Pittsburgh, PA: CERT/Carnegie Mellon. Retrieved from www.cert.org/archive/pdf/11tn006.pdf.

Holt, T. J. and Graves, D. C. (2007). A qualitative analysis of advanced fee fraud schemes. *The International Journal of Cyber Criminology 1*(1), 137-154.

Holt, T. J. and Lampke, E. (2010). Exploring stolen data markets on-line: Products and market forces. *Criminal Justice Studies, 23,* 33-50.

Identity Theft Resource Center. (2009). *Identity theft: The aftermath 2008*. San Diego, CA: Author. Retrieved from http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2008_20090520.pdf.

Identity Force. (2009). *Red flags rules: Hospital compliance report as data breaches increases, dentity theft prevention programs continue to challenge hospitals*. Retrieved from http://www.identityforce.com/tools/downloads/FINAL_IDF_RFRF_report pdf.

ID Experts. (2009). 2009 *HIMSS analytics report: Evaluating HITECH's impact on healthcare privacy and security*. Retrieved from http://www.himssanalytics.org/docs/ID_Experts_111509.pdf.

Javelin Strategy & Research (2008). *2008 Identity Fraud Survey Report*. Retrieved from https://www.javelinstrategy.com/news/831/92/Javelin-Research-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail.

Javelin Strategy & Research. (2009). *2009 Identity fraud survey report: Consumer versionprevent-detect-resolve*. Retrieved from https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraud SurveyConsumer.pdf.

Jones, V. (2008). *Requirements for personal information protection part 1: U.S. federal law*. Pittsburg, PA: ARMA International Educational Foundation. Retrieved from http://www.armaedfoundation.org/pdfs/FederalPrivacy.pdf.

Jordan, T. and Taylor, P. (1998). A sociology of hackers. *Sociological Review, 46*(4), 757-780.

King, R. (2011, Sept. 7). *IBM panel discusses tackling big data storage as problem escalates*. Retrieved from http://www.smartplanet.com/blog/smart-takes/ibm-panel-discusses-tackling-big-data-storage-as- problem-escalates/19010.

Kowalski, E., Cappelli, D., and Moore, A. (2008). *Insider threat research: Illicit cyberactivity in the information technology and telecommunications sector*. USSC & Carnegie Mellon University. Retrieved from www.cert.org/archive/pdf/insiderthreat_it2008.pdf.

Kroll Advisory Solutions (2012). *2012 HIMSS analytics report: Security of patient data*. Retrieved from http://www.krollcybersecurity.com/media/Kroll-HIMSS_2012_Security_of_Patient_Data_040912.pdf.

Lai, F., Li, D., and Hsieh, C. (2012). Fighting identity theft: The coping perspective decision support system, *Decision Support Systems*, 52, 353-363.

Mearian, L. (2011, June 28). *World data will grow by 50X in next decade, IDC Research predicts*. Retrieved from http://www.computerworld.com/s/article/9217988/World_s_data_will_grow_by_50Xin_next_decade_IDC_research_predicts.

McNally, M. and Newman, G. (2008). *Perspectives on identity theft*. Monsey, NY: Criminal Justice Press.

Michael, H. (2011). *Deriving Candidate Technical Controls and Indicators of Insider Attack From Socio-Technical Models and Data*. Pittsburgh, PA: Carnegie Mellon University. Retrieved from http://www.sei.cmu.edu/library/abstracts/reports/11tn003.cfm.

National Cybersecurity and Communications Integration Center (2012). *Attack surface: Healthcare and public health sector: Executive overview*. Retrieved from http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf.

Newman, G.R. and Clarke, R.V. (2003). *Superhighway robbery: Preventing e-Commerce crime*. Cullompton, U.K.: Willan Press.

Newman, G. R. (2004). *Identity theft: Guide no. 25*. Washington, DC: Center for Problem-Oriented Policing. Retrieved from http://www.popcenter.org/Problems/problem-identity_theft.htm.

Newman, G. R. and McNally, M. (2005). *Identity theft literature review*. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf.

Newman, G.R. (2009). Policy thoughts on “Bounded rationality of identity thieves.” *Criminology & Public Policy*. *8*(2). 271-278.

Office of Community Oriented Policing Services. (2006). *A national strategy to combat identity theft*. Washington, DC: Department of Justice. Retrieved from www.cops.usdoj.gov/Publications/e03062303.pdf.

Ponemon Institute. (2005). *National survey on data security breach notification.* Retrieved From *http://www.whitecase.com/files/FileControl/863d572d-cde3-4e33-903c-37eaba537060/7483b893-e478-44a4-8fed-f49aa917d8cf/Presentation/File/Security_Breach_Survey%5B1%5D.pdf.*

Ponemon Institute. (2011a). *2011 Cost of a data breach research*. Retrieved from www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf.

Ponemon Institute. (2011b). *Reputation impact of a data breach executive summary*. Retrieved from http://media.scmagazineus.com/documents/30/ponemon_reputation_ impact_of_a_7405.pdf.

Ponemon Institute. (2012a). *Aftermath of a data breach research*. Retrieved from http://www.experian.com/assets/data-breach/brochures/ponemon-aftermath-research.pdf.

Ponemon Institute. (2012b). *Third annual survey on medical identity theft*. Retrieve from http://www.ponemon.org/local/upload/file/Third_Annual_Survey_on_ Medical _Identity_Theft_FINAL.pdf.

Pontell, H.N. (2009). Identity theft: Bounded rationality, research, and policy. *Criminology & Public Policy*. *8*(2). 263-270.

Pontell, H. N., Brown, G. C., and Tosouni, A. (2008). Stolen identities: A victim survey. In G. Newman & M. McNally (Eds.). *Crime Prevention Studies: Identity Theft and Opportunity* (pp. 57-86). New York, NY: Criminal Justice Press.

Rapid7. (2012). *Rapid7 Report: Data breaches in the government sector*. Retrieved from http://www.rapid7.com/docs/data-breach-report.pdf.

Roberds,W. and Schreft, S. (2009). Data breaches and identity theft. *Journal of Monetary Economics*, *56*(7), 918-929.

Rebovich, D. (2009). Examining identity theft: Empirical explorations of the offense and the offender. *Victims and Offenders*, *4*, 357−364.

Reisig, M. D., Pratt, T., and Holtfreter, K. (2009). Perceived risk of internet theft victimization. *Criminal Justice and Behavior*, *36*, 369-384.

Romanosky, S., Telang, R., and Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*(2), 256-286.

Schreft, S.L. (2007). *Risks of identity theft: Can the market protect the payment system?* Kansas City, KS: The Federal Reserve Bank of Kansas City. Retrieved from http://www.kansascityfed.org/Publicat/ECONREV/PDF/4q07Schreft.pdf.

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., and Shimeall, T.J. (2012). *Common sense guide to mitigating insider threats (4th Edition)*: Technical report. Pittsburgh, PA: Carnegie Mellon University. Retrieved from www.sei.cmu.edu/reports/12tr012.pdf.

Synovate. (2003). *Federal Trade Commission-Identity theft survey report*. McLean, VA: Author. Retrieved from http://www.ftc.gov/os/2003/09/synovatereport.pdf.

Synovate. (2007). *Federal Trade Commission 2006 identity theft survey report*. McLean, VA: Author. Retrieved from http://www.search.org/files/pdf/synovatereport.pdf.

Stevens, G. (2010). *Federal information security and data breach notification laws*. Washington, D.C.: Congressional Research Service. Retrieved from www.fas.org/sgp/crs/secrecy/RL34120.pdf.

Symantec. (2012). *State of information global results*. Retrieved from http://www.symantec.com/content/en/us/about/media/pdfs/2012-state-of-information-global.en-us.pdf.

Telang, R. and Wattal, S. (2005). *Impact of software vulnerability announcements on the market value of software vendors- an empirical investigation*. Pittsburgh, PA: Carnegie Mellon University. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=677427.

The College Board (2012). *2012 College Handbook (49th edition)*. New York, NY: Author.

The Office of Management and Budget. (2012). *Fiscal year 2011 report to Congress on the implementation of the federal information security management act of 2002*. Washington, DC: Author. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy11_fisma.pdf.

The Office of Management and Budget. (2013). *Fiscal year 2011 report to Congress on the implementation of the federal information security management act of 2002*. Washington, DC: Author. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

Thomas, R. and Martin, J. (2006). The underground economy: Priceless. *The Usenix Magazine*. *31*(6), 7-17. Retrieved from http://static.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf.

U.S. Government Accountability Office. (2007). *Personal information: Data breaches are frequent, but evidence of resulting identity theft are limited; however, the full extent is unknown*. Washington, DC: Author. Retrieved from http://www.gao.gov/new.items/d07737.pdf.

U.S. Government Accountability Office. (2011). *Cybersecurity: Continued attention needed to protect our nation's critical infrastructure*. Washington, DC: Author.
Retrieved from http://www.gao.gov/new.items/d11865t.pdf.

U.S. Government Accountability Office. (2011). *Information security: Weaknesses continue amid new federal efforts to implement requirements*. Washington, DC:
Author. Retrieved from http://www.gao.gov/new.items/d12137.pdf.

U.S. Government Accountability Office. (2011). *Taxes and identity theft: status of IRS initiatives to help victimized taxpayers*. Washington, DC: Author. Retrieved
from http://www.gao.gov/assets/130/126293.pdf.

U.S. Government Accountability Office. (2012). *Cybersecurity threats impacting the nation*. Washington, DC: Author. Retrieved from http://www.gao.gov/assets/ 600/590367.pdf.

Verizon, Inc. (2012). *2012 Data breach investigations report*. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

Wade, C., Aldridge, J., Hopper, L., Drummond, H., Hopper, R., and Andrew, K. (2011). Hacking into the hacker: separating fact from fiction. . In T.J. Holt (Ed.).
Crime on-line: Correlates, causes and context (pp. 29-56). Carolina Academic Press: Durham, North Carolina.

Zhang, L., Young, R., and Prybutok, V. (2007). Inhibitors of two illegal behaviors: hacking and shoplifting. *Journal of Organizational and End User Computing*. *19*(3), 24-33.

APPENDICES

Appendix I: Information Theft Rates by Industrial Sector and Type of Incident

Sector	Industrial category	Total Firms	Hacking	Hacking Rate	Inside Theft	Insider Rate
Business	Utilities (Energy)	5,824	7	0.120	6	0.103
	Manufacturing	256,363	77	0.030	25	0.010
	Retail/Whole sale Stores	817,819	159	0.019	54	0.007
	Car Dealer	81,450	2	0.002	12	0.015
	Gas station	66,511	2	0.003	10	0.015
	Transportation	168,057	8	0.005	6	0.004
	Publishing/Web Service/Software	27,612	43	0.156	1	0.004
	Broadcasting/Media	4,682	13	0.278	6	0.128
	Telecommunications/ Internet Service	8,584	25	0.291	26	0.303
	Data Processing	9,580	44	0.459	7	0.073
	Bank	13,463	66	0.490	61	0.453
	Financial Service	58,912	88	0.149	47	0.080
	Insurance	134,576	29	0.022	31	0.023
	Tax Service	112,301	11	0.010	14	0.012
	Professional Service	291,152	56	0.019	30	0.010
	Administrative and Support Services	309,657	18	0.006	13	0.004
	Hotel	52,119	37	0.071	12	0.023
	Food Service	443,569	73	0.016	51	0.011
Education	Higher Education	4,599	171	3.718	22	0.478
Medical	Hospital by AHA 2014	5,723	25	0.440	135	2.359
	Medical/Health Service	431,305	26	0.006	48	0.011
	Nursing/Social Service	211,258	10	0.005	13	0.006
Governmental	Federal	479	31	6.472	35	7.307
	State	51	46	76.5	66	47.1
	City	289	15	5.190	22	7.612
	Local	38,621	32	0.083	28	0.072

* Professional Service: Computer system design, Management, Scientific and Technical Consulting service, Advertising and Public relations

* Theft rates of state governments: Dividing total incidents by 51 state governments.

Appendix II: IT Security Incidents at the 24 Federal Agencies in 2012-2013

No.	Department	Average Total	Equipment	Policy Violation	Non Cyber	Suspicious Network Activity	Un-authorized Access	Denial of Service	Malicious Code	Improper Usage	Social Engineering	Other
		52,095	8,441	10,162	13,965	2,428	490	40	8,775	826	2,984	4,036
1	Veterans	9,995	2016	2467	4271	139	33	2	824	4	63	179
2	H & H Services	6,201	910	1318	977	195	158	1	1576	1	793	275
3	NASA	5,247	393	87	10	120	91	5	1668	2	772	2101
4	SSA	4,770	56	114	4489	79	3	0	3	0	0	26
5	Justice	4,358	2026	481	155	72	11	12	861	593	55	93
6	Defense	3,712	311	2002	1187	57	12	0	10	11	21	104
7	Treasury	3,396	805	563	1667	128	1	0	191	2	10	30
8	Homeland S.	2,632	119	916	238	128	27	4	580	137	85	400
9	Trans. D.	2,578	135	449	16	330	28	1	1285	2	104	232
10	Commerce	1,879	511	344	133	223	33	4	385	7	76	166
11	State	1,469	6	48	477	87	3	0	16	1	776	55
12	Agriculture	1,453	349	93	28	165	7	1	721	2	35	55
13	Energy	1,092	280	122	21	89	30	2	278	41	80	150
14	Interior	1,034	17	854	15	107	2	0	10	0	5	25
15	GSA	445	209	29	3	67	6	2	103	1	6	22
16	H & UD	434	178	26	2	53	5	0	77	0	58	38
17	Education	324	13	77	89	60	28	3	39	0	3	15
18	OPM	238	12	33	116	68	1	1	0	0	1	8
19	EPA	190	3	11	11	84	4	1	51	1	3	24
20	USAID	188	16	45	2	23	2	0	85	6	2	10
21	Labor	178	23	18	51	73	2	1	3	0	1	8
22	NRC	136	48	20	3	2	2	0	5	15	33	10
23	SBA	98	4	43	3	45	0	0	1	0	1	3
24	NSF	48	1	2	1	34	1	0	3	0	1	7

Source: Compiled from the Whitehouse FISMA reports (2012 and 2013).

Appendix III: FISMA Capabilites Evalutation Metrics in 2010-2013

Category	Capability Area	FY 2010	FY2011	FY 2012	FY 2013
Continuous Monitoring Capabilities	Automated Asset Management	66%	80%	86%	83%
	Automated Configuration Management	50%	78%	70%	79%
	Automated Vulnerability Management	51%	77%	83%	81%
Trusted Internet Connections (TIC)	TIC Traffic Consolidation	48%	65%	81%	86%
	TIC 2.0 Capabilities	60%	72%	84%	87%
Strong Authentication	PIV Logical Access	55%	66%	57%	67%
Portable Device Encryption	Portable Device Encryption	54%	83%	90%	84%
DNSSEC & Email Validation	DNSSEC Implementation	35%	65%	74%	93%
	E-mail Validation Technology	46%	58%	64%	74%
Remote Access	Remote Access Authentication	52%	52%	53%	79%
	Remote Access Encryption	72%	83%	82%	98%
Controlled Incident Detection	Controlled Incident Detection	70%	49%	63%	73%
Security Training	User Training	92%	99%	88%	94%
	User with Security Responsibility Training	88%	92%	92%	92%
Automated Detection and Blocking of Unauthorized Software	Detect and Block Unauthorized Software	N/A	N/A	60%	73%
Email Encryption	Email Encryption	N/A	N/A	35%	51%
Government-wide Average		62%	74%	74%	81%

Source: Compiled from the Whitehouse reports in 2011-2013.

Appendix IV: FISMA Capabilities Evaluations among 24 Federal Agencies 2013

Agency	Continuous Monitoring	Trusted Internet Connection	Authentication	Encrypted Portable Device	DNSSEC/ Email Validation	Remote Access	Controlled Incident Detection	Security Training	Automated Capabilities to detect and block unauthorized	Encrypted Email system
VA	92.00	80.00	42.84	84.00	48.00	51.00	94.00	99.67	31.50	50.00
HHS	78.44	47.84	48.00	84.33	73.33	78.34	7.00	94.34	50.50	76.50
NASA	82.78	84.00	46.17	50.00	100.00	87.67	58.67	98.50	10.50	100.00
SSA	84.78	98.67	50.00	97.33	100.00	98.84	30.00	98.50	50.00	100.00
Justice	85.66	96.34	30.50	93.67	89.00	100.00	100.00	98.34	94.50	100.00
DOD	81.33	na	50.67	88.67	56.34	79.33	66.67	93.00	86.00	85.00
Treasury	76.11	84.50	46.17	99.00	54.67	84.84	61.67	98.34	37.00	19.50
DHS	80.56	94.17	47.50	78.67	84.84	60.50	100.00	88.67	54.00	0.00
DOT	56.22	88.00	45.17	87.67	71.17	49.50	85.00	92.67	59.50	41.00
Commerce	61.56	52.17	41.00	85.67	61.34	82.84	50.33	92.50	42.50	27.00
State	67.89	94.00	50.00	86.00	66.67	100.00	16.67	68.50	60.50	5.00
USDA	90.66	83.83	38.34	77.00	55.84	58.17	44.00	98.83	50.00	100.00
Energy	73.55	61.84	42.00	64.33	53.50	86.17	96.33	88.67	62.00	38.00
Interior	74.44	79.00	43.84	73.33	74.84	55.00	83.00	90.33	25.00	15.00
GSA	96.55	33.33	45.59	99.33	79.34	85.34	66.33	91.84	95.50	1.00
HUD	83.78	88.67	50.00	93.33	47.67	61.17	na	79.00	62.50	35.00
ED	88.22	87.84	48.17	100.00	97.84	83.34	96.67	97.34	100.00	0.00
OPM	85.55	92.17	45.67	97.33	100.00	91.67	66.67	92.17	99.50	100.00
EPA	63.89	96.00	49.00	85.33	38.34	83.34	0.00	95.67	17.50	0.50
USAID	85.44	98.67	29.50	91.67	83.83	100.00	38.33	80.34	50.00	25.00
Labor	83.67	55.34	40.00	99.33	93.84	94.67	66.67	94.17	91.50	22.00
NRC	96.56	66.67	50.00	100.00	87.50	94.34	50.00	74.17	29.00	100.00
SBA	63.44	66.67	24.50	62.33	66.67	59.50	100.00	92.67	95.50	0.00
NSF	96.67	97.17	50.00	93.67	72.17	100.00	33.33	96.84	80.50	0.00

Source: Compiled from the Whitehouse FISMA reports (2012 and 2013), Unit: %.

Appendix V: Processes of Information Theft by Hacker

Step	Individual	Organizations	Hacker	Law Enforcement
1	Information created.			
2	Information provided to organization.	Information received and stored.		
3		Information protected.		
4			Hacker's need is created.	
5			Vulnerable target is searched.	
6			Target is selected by hacker's choice.	
7		Hacking is detected and blocked.	1. Hacker intruded into an organization. 2. Intrusion is failed.	
8		Monitoring is strengthened.	Data and information is accessed and stolen (copied, transferred or altered).	
9			Information is obtained by a hacker.	
10			Information is processed for criminal purposes. (i.e. hacking result is posted, data is sold in underground market, or misused for fraud).	
11			Criminal benefits are obtained (i.e. monetary profit or hacker's reputation).	
12	Incident is detected and reported to organization or LE agency.	1. Incident is detected. 2. Damage is estimated. 3. Remedy measure is taken. 4. Reported to customer and LE agency.		Incident is reported from victim (customer or organization).
13	Updated information is used (i.e. new credit card and new PIN number is reissued).			Investigation is initiated.
14				1. No arrested is made by technical or legal limitations. 2. Arrest is made.
15		1. New protection program is installed. 2. Awareness training is held.	1. Hacking is stopped by arrest. 2. Seeking for another targets.	Public awareness events will be held (i.e. statistics release or conferences).
16			New hacking skill is developed for a newly installed protection program at organizations.	

Appendix VI: Processes of information Theft by Insider

Step	Individual	Organization	Inside Offender	Law Enforcement
1			Employed earlier.	
2	Information created.			
3	Information provided to organization.	Information received and stored.		
4		Information protected.	Information managed by employees.	
5			Insider offender's need is created.	
6			Target information is selected.	
7			Vulnerable environments and time are selected.	
8			Data and information is accessed and stolen (copied, transferred or altered).	
9			1. Information is obtained by inside offender. 2. Offender leaves the organization for a new job with stolen information.	
10			Information is processed for criminal purposes. (i.e. Sold in underground market, or misused for fraud).	
11			Criminal benefits are obtained (i.e. monetary profits).	
12	Incident is detected and reported to organization or LE agency.	1. Incident is detected. 2. Damage is estimated. 3. Remedy measure is taken. 4. Reported to customer and LE agency.	Employment is continued	Incident is reported from victim (individual or organization).
13	Updated information is used (i.e. new credit card and new PIN number is reissued).			Investigation is initiated.
14			Future offense is stopped or resumed.	1. No arrested is made. 2. Arrest is made.
15		1. New protection program is installed. 2. Awareness training Is held.		Public awareness events will be held (i.e. statistics release or conferences).

Appendix VII
Opportunity-Reducing Techniques in Information Theft Environment (1-15)

Increase the Perceived Effort				
1. Harden targets	**2. Control access to facilities**	**3. Screen exits**	**4. Deflect Offenders**	**5. Control tools/weapons**
- Operate a high level of IT security management. - Separate the IT system network from outer internet. - Monitoring of accesses to customer data.	- Operate dual sign-ups to access data. - Record the copied documents - Keep records of access by employees and customers. - Assign “Authorized persons only” places. - Operate CC-TVs. - Issue biometric pass.	- Keep records of access. - Operate CC-TVs - Keep records at entrances and exits. - Patrol inside of the facilities.	- Keep records of log-ins. - Use digital certificates* - Install biometric authentication* - Analyze user patterns to detect deviant use*	- Operate dual sign-ups to access data. - Record copied documents. - Monitor computer viruses. - Keep data encrypted - Keep data confidential - Secure back-up data

Increasing the Received Risks				
6. Extend guardianship	**7. Assist natural surveillance**	**8. Reduce anonymity**	**9. Utilize place managers**	**10. Strength formal surveillance**
- Update security hardware & software on time. - Perform peer evaluations for security performances.	- Set up a hotline with law enforcement agencies - Check credits reports & billing statement. - Contract external security audit company.	- Install employee signature embedded in electronic documents	- Hold awareness campaigns. - Train all employees in correct security procedures.* - Offer incentives for employee vigilance.*	- Install CC-TVs at major exits. - Include regular employees in security team.*

Reduce the Rewards				
11. Conceal targets	**12. Remove targets**	**13. Identify property**	**14. Disrupt markets**	**15. Deny benefits**
- Keep valuable databases offline*- Keep data encrypted. - Keep data confidential		Display prominently copyright material on software and other electronic products*	Strengthen cyber-patrols about underground market.	Inform liability cases to retiring employees.

* Newman & Clarke (2003)

Opportunity-Reducing Techniques in Information Theft Environment (16-25)

Reduce Provocations				
16. Reduce frustration & stress	**17. Avoid disputes**	**18. Reduce emotional arousal**	**19. Neutralize peer-pressure**	**20. Discourage imitation**
- Provide benefits to IT security staff. - Providing job stress counseling.	Provide trainings for protecting data.	- Repair immediately damage to system* - Limit publicity about new security* - Regulate fraudulent advertising and scam websites* - Install embedded signature in electronic document/printed documents.	Hold awareness campaigns.	Update security hardware & software patches on time.

Remove the Excuses				
21. Set rules	**22. Post instructions**	**23. Alert conscience**	**24. Assist compliance**	**25. Control drug/alcohol**
- Develop manuals for data protecting policy. - Establish contingency plan against cyberattacks.	- Place slogans for protecting data. - Display tags of copyright-protected products.	- Place sigh board "Protect your data." - Provide trainings for protecting data.	- Inform simple and clear procedures about data security to employees. - Provide benefits to employees who follow security procedures.	- Present awareness campaigns.

* Newman & Clarke (2003)