

2009

An Analysis of the Impact of Information Security Policies on Computer Security Breach Incidents in Law Firms

Faith M. Heikkila

Nova Southeastern University, fheikkila@charter.net

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd

 Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

NSUWorks Citation

Faith M. Heikkila. 2009. *An Analysis of the Impact of Information Security Policies on Computer Security Breach Incidents in Law Firms*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (176)
https://nsuworks.nova.edu/gscis_etd/176.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

An Analysis of the Impact of Information Security Policies
on Computer Security Breach Incidents in Law Firms

by
Faith M. Heikkila

A dissertation submitted in partial fulfillment of the requirements
for the Degree of Doctor of Philosophy
in
Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

2009

We hereby certify that this dissertation, submitted by Faith M. Heikkila, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Marlyn Kemper Littman, Ph.D.
Chairperson of the Dissertation Committee

Date

Maxine Cohen, Ph.D.
Dissertation Committee Member

Date

Ling Wang, Ph.D.
Dissertation Committee Member

Date

Approved:

Amon Seagull, Ph.D.
Interim Dean, Graduate School of Computer and Information Sciences

Date

Graduate School of Computer and Information Sciences
Nova Southeastern University

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An Analysis of the Impact of Information Security Policies
on Computer Security Breach Incidents in Law Firms

By
Faith M. Heikkila

2009

Law firms maintain and store voluminous amounts of highly confidential and proprietary data, such as attorney-client privileged information, intellectual properties, financials, trade secrets, personal, and other sensitive information. There is an ethical obligation to protect law firm client data from unauthorized access. Security breaches jeopardize the reputation of the law firm and could have a substantial financial impact if these confidential data are compromised. Information security policies describe the security goals of a law firm and the acceptable actions and uses of law firm information resources.

In this dissertation investigation, the author examined the problem of whether information security policies assist with preventing unauthorized parties from accessing law firm confidential and sensitive information. In 2005, Doherty and Fulford performed an exploratory analysis of security policies and security breach incidents that highlighted the need for research with different target populations. This investigation advanced Doherty and Fulford's research by targeting information security policies and security breach incidents in law firms. The purpose of this dissertation investigation was to determine whether there is a correlation between the timing of security policy development (proactive versus reactive policy development) and the frequency and severity of security breach incidents in law firms of varying sizes.

Outcomes of this investigation correlated with Doherty and Fulford's general findings of no evidence of statistically significant relationships between the existence of a written information security policy and the frequency and severity of security breach incidents within law firms. There was also a weak relationship between infrequency of information security policy updates and increase of theft resources. Results demonstrated that, generally, written information security policies in law firms were not created in response to a security breach incident. These findings suggest that information security policies generally are proactively developed by law firms.

Important contributions to the body of knowledge from this analysis included the effectiveness of information security policies in reducing the number of computer security breach incidents of law firms, an under represented population, in the information assurance field. Also, the analysis showed the necessity for law firms to become more immersed in state security breach notification law requirements.

Acknowledgments

Dr. Littman has been a very big supporter of my publications and dissertation process as my Dissertation Advisor. She has helped me to become a much better writer than when I first started the doctoral program. I am extremely grateful for her wonderful support and encouragement along this incredibly long path. Also, I am very grateful to have the opportunity to have Dr. Cohen and Dr. Wang participate as members of my Dissertation Committee. Their insight and suggestions were very helpful in producing a much better product.

I truly appreciate all of the support I received from Randi Mayes, the ILTA Executive Director, who assisted me with the distribution of my survey to the ILTA members. From the first time I approached Randi back in the beginning of my doctoral studies to the final distribution of my survey, she has shown me the utmost support and encouragement. Thank you for everything you have done for me. I also appreciate the support the ILTA Past Presidents, Judi Flournoy and Joy Heath Rush, provided and thank you for all the sage advice you gave me.

I am forever mindful that those we surround ourselves with have much to impart in the way of wisdom and knowledge. As such, I was able to call on a few very good friends who also happen to be experts in their field. Thank you so very much, Mark Thorogood, for supporting me on this journey from the first time I met you in class to the many trips to Chicago where I picked your brain. Ruth Stevens, thank you for your support and for all the helpful insight you provided. I also want to thank Dr. Anne Abatte for her wonderful assistance with their review of my survey. A special thank you to Dr. Phyllis Curtiss and the Grand Valley State University Statistical Consulting Center for their magnificent assistance with the statistics.

My good friend, Meg Hackett, Esq., an attorney with whom I used to work helped propel me over the final hurdle with her words of wisdom in the form of reviewing my dissertation from a lawyer's viewpoint. I appreciate the time you took to carefully review my work and to provide such incredible insight. Terri Tomaszek, Ph.D. was always such a positive influence in this journey. Thank you for taking the time to come down and go through my revisions to make sure I was on the right page.

To Regan Fader, I want to express my heartfelt gratitude for your integral support in the terms of financial and emotional support. I especially loved the pigtails and pom poms when I felt down or paralyzed by the enormity of the task! You were and are a great supporter of my work and a highly intelligent person to discuss my ideas with throughout this quest. You certainly are the one who really got me through this incredible journey. Thank you so much for the wonderful, faithful, kind, and loving remarks you gave to me throughout all these years of studying, writing, writhing, crying, and joyful moments we have shared during this process. You have been a true trooper and I will never forget how devoted to the cause you were with me.

I want to dedicate this dissertation to my dear, sweet mother who was always a role model for me. As a child, I observed and admired her leadership in the various women's groups she led. As an adult, I was so very proud of her and how courageously she faced her Alzheimer's to the very end. I love you and miss you.

Table of Contents

Abstract iii
List of Tables vii
List of Figures xi

Chapters

1. Introduction 1

Problem Statement and Goal 5
 Problem Statement 5
 Goal 6
Relevance, Significance, and Need for the Study 8
Barriers and Issues 12
Research Questions Investigated 13
Limitations and Delimitations of the Study 15
Definition of Terms 16
Summary 20

2. Review of the Literature 22

Introduction 22
The Theory and Research Literature Specific to the Topic 22
 Security Policies 22
 U.S. Data Privacy Laws 28
 Security Data Breach Notification Laws 29
 U.S. Identity Theft Regulations 33
 Identity Theft Red Flags Rule 35
 PCI DSS (PCI Data Security Standards) 38
 Health Insurance Portability and Accountability Act (HIPAA) of 1996 38
International Data Privacy Laws 40
 European Union (EU) Privacy Laws 41
 Canadian Privacy Laws 42
 Safe Harbor 43
Data Leakage Threats 43
Insider Threats 44
Data Breach Incidents 48
Information Security Assessment 54
 Management Controls 58
 Operational Controls 60
 Technical Controls 62
Summary of What is Known and Unknown about the Topic 63
The Contribution This Study Will Make to the Field 64

3. Methodology 67

Research Methods Employed	67
Specific Procedures Employed	68
Online Survey Development and Distribution	68
Sampling and Participants	71
Data Collection	73
Data Analysis	73
The Role of the Researcher	74
Reliability and Validity	75
Threats to Internal Validity	85
Threats to External Validity	86
Formats for Presenting Results	86
Resource Requirements	87
Summary	87

4. Results 89

Introduction	89
Findings	92
Demographic Analysis	92
Law Firm Demographics	94
Follow-Up Questions	98
Survey Data Analysis	100
Research Questions Answered	102
Summary of Results	139

5. Conclusions, Implications, Recommendations, and Summary 142

Conclusions	142
Strengths of Study	155
Limitations	156
Implications	157
Recommendations	160
Summary	162

Appendixes

A. Permissions	168
B. List of Acronyms	172
C. IRB Approval	175
IRB Amendment Approval	176
D. ILTA Letter of Understanding and Authorization	177
E. Survey Instrument to ILTA Members	178
F. Doherty & Fulford Original Survey Instrument	193
G. Revised Doherty & Fulford Original Survey Instrument	197

Reference List 201

List of Tables

Tables

1. Differences Within the State Security Breach Notification Laws 31
2. Summary of 656 Data Breaches 51
3. Variables, Research Questions, and Items on Author's Survey 69
4. Feedback from the Subject Matter Experts That Served as Panel Members 76
5. Open Ended Follow-Up Questions 91
6. Demographic Data of the Study Respondents 92
7. Size of Law Firm in Number of Users of the Study Respondents 94
8. Size of Law Firm Information Technology Department of the Study Respondents 95
9. Location of Law Firm Offices of the Study Respondents 95
10. Region Where Law Firm Offices of the Study Respondents Were Based 96
11. Functions of the Law Firm Technology-related Departments of the Study Respondents 96
12. Law Firm Designation of Security Personnel of the Study Respondents 97
13. Law Firm Respondents' Designation of Responsibility for Information Security 97
14. Privacy and Security Laws Identified by Law Firm Respondents for Compliance 98
15. Region Where Law Firm Offices of the Follow-up Respondents Were Based 100
16. U.S. Security Breach Notification Laws 100
17. Doherty & Fulford Table 2. The Incidence and Severity of Security Breaches 101
18. Law Firms – Incidence and Severity of Security Breaches 101
19. Doherty & Fulford – Table 3 The Relationship Between the Adoption of Information Security Policy and the Incidence and Severity of Security Breaches 103
20. Law Firms – Relationship Between the Adoption of Information Security Policy and the Incidence and Severity of Security Breaches 104

21. Doherty & Fulford – Table 4. Relationship between the Age of Information Security Policy and the Incidence/Severity of Security Breaches 105
22. Law Firms – Relationship Between the Age of Information Security Policy and the Incidence/Severity of Security Breaches 105
23. Doherty & Fulford – Table 5. Relationship Between the Frequency of Updating the Information Security Policy and the Incidence/Severity of Security Breaches 106
24. Law Firms – Relationship Between the Frequency of Updating the Information Security Policy and the Incidence of Security Breaches 107
25. Law Firms – Relationship Between the Frequency of Updating the Information Security Policy and the Incidence/Severity of Security Breaches 107
26. Doherty & Fulford – Table 6. Relationship Between the Range of Issues Covered by the Information Security Policy and the Incidence/Severity of Security Breaches 108
27. Law Firms – Relationship Between the Range of Issues Covered by the Information Security Policy and the Incidence/Severity of Security Breaches 109
28. Doherty & Fulford – One-way ANOVA between the Successful Adoption of Success Factors and the Incidence/Severity of Security Breaches 110
29. Law Firms – Spearman’s Rho Between the Successful Adoption of Success Factors and the Incidence/Severity of Security Breaches 110
30. Law Firm – Success Factors’ Importance of Best Practices 111
31. Law Firm – Success Factors’ Adoption of Best Practices 112
32. Law Firms – Cronbach Alpha Internal Reliability Test of 10 Success Factors 113
33. Law Firm Computers Shut Down for Inactivity After A Defined Period 113
34. Law Firm – Security Issues Covered in IT Security Policies and/or Separate Procedures or Standards 114
35. Law Firms – IT Security Policy Documents Approved By Management 114
36. Communication of Law Firm Approved IT Security Policy Documents 115
37. Publication of Law Firm IT Security Policy Documents 115

38. Law Firm Employees/Lawyers Under a Time Deadline to Finish an Assignment – Use of Security Measures 116
39. Law Firm Employees/Lawyers Under a Time Deadline to Finish an Assignment – Scan a File for Viruses 116
40. Law Firm Employees/Lawyers Under a Time Deadline to Finish an Assignment – Install Security Software Updates 117
41. Law Firm Employees/Lawyers Under a Time Deadline to Finish an Assignment – Install a Digital Certificate 118
42. Law Firm Employees/Lawyers Under a Time Deadline to Finish an Assignment – Install An ActiveX Control From An Unknown Source 118
43. Law Firm Size in Number of Users and Existence of a Security Policy 119
44. Law Firms – Spearman’s Rho Between the Internet’s Effect on Breaches and the Need for Policies 120
45. Law Firm – Attorney-Client Work Product Communication Over Electronic Networks 121
46. Law Firm – Performance of Security Tasks During the Past 12 Months 121
47. Law Firms – Spearman’s Rho Between the Law Firm Size and Each Pair of Variables 123
48. Law Firms Grouped – Law Firm Size and Perform a Vulnerability Assessment 124
49. Law Firm Size and Perform a Vulnerability Assessment 125
50. Law Firms Grouped – Law Firm Size and Hiring of An Outside Consultant 125
51. Law Firm Size and Hiring of An Outside Consultant 126
52. Law Firms Grouped – Law Firm Size and In-House Risk Assessment 127
53. Law Firm Size and In-House Risk Assessment 128
54. Law Firms Grouped – Law Firm Size and Employee Training 128
55. Law Firm Size and Employee Training 129
56. Law Firms Grouped – Law Firm Size and Third Party Service 130

57. Law Firm Size and Third Party Services	130
58. Law Firms Grouped – Law Firm Size and Encrypt E-mail Messages	131
59. Law Firm Size and Encrypt E-mail Messages	131
60. Law Firms Grouped – Law Firm Size and Encrypt Hard Drive Data	132
61. Law Firm Size and Encrypt Hard Drive Data	132
62. Law Firms Grouped – Law Firm Size and Review of Information Security Policies	133
63. Law Firm Size and Review of Information Security Policies	134
64. Law Firms Grouped – Law Firm Size and Revise Information Security Policies	135
65. Law Firm Size and Revise Information Security Policies	135
66. Law Firm Size and Audit and Enforce Document IT Security Policy	136
67. Law Firm Size and IT Security Policy Audited By Independent Third Party	136
68. Law Firm Size and Dissemination of the Security Policy	137
69. Law Firm Groups – Law Firm Size and Written Information Security Policy	138
70. Small vs. Very Large Law Firm and Written Information Security Policy	138
71. Small vs. Very Large Law Firm and Information Security Breach Incidents	139

List of Figures

Figures

1. States with security breach laws map 30
2. Incidents by sector 48
3. Incidents by data type 49
4. Incidents by breach type 50
5. How data are breached 52

Chapter 1

Introduction

Introduction

Law firms are entrusted with highly confidential and privileged client documents containing personal data that may include financial, shareholder, personally identifiable information (PII), trade secrets, and/or attorney-client privileged information. Reinstein and Seward (2008) define attorney-client privileged information as confidential communications between clients and their attorneys to allow truthful disclosure when seeking legal advice that cannot be discovered by other parties, including adverse parties in lawsuits. Law firms have an obligation to maintain, store, and secure this sensitive information and to ensure their clients' privacy (Comerford, 2006; Nelson, Isom, & Simek, 2006). Security breaches are incidents consisting of unauthorized access to sensitive or confidential data of the law firm (Kraemer & Carayan, 2007; Schwartz & Janger, 2007; Silverman, 2007). Information security policies describe the security goals and procedures of a law firm (Da Veiga & Eloff, 2007; Metzler, 2007; Robinson, 2005).

Information security policies are specifically designed to safeguard network resources from security breaches (Doherty & Fulford, 2005). Information security policies outline the responsibilities and acceptable use actions of law firm employees (Baker & Wallace, 2007; Ries, 2007) when using law firm computers and networks. Security controls include management controls, operational controls, and technical controls. Information

security policies are considered management controls and define appropriate security of the network infrastructure (Post & Kagan, 2007). Incorporated in the security policy is a clear explanation of the rules with regard to how the network can be accessed, with a concentration on maintaining confidentiality and identifying the ramifications of a security breach (Greene, 2006; Whitman & Mattord, 2008). Other management controls include vulnerability assessments and security plans implemented to manage the security (Bowen, Hash, & Wilson, 2006; Salmela, 2008) of the law firm. Operational controls include physical security, personnel security, business continuity planning, incident response, hardware and software maintenance, confidential data protection, and security awareness training (Bowen, et al.; Hagen, Albrechtsen, & Hovden, 2008) that are implemented by law firm personnel rather than automatically by computer software.

Technical controls include firewalls, anti-virus, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and access controls. Farn, Lin, and Lo (2008) define defense-in-depth as a way to overlap security policies, technical controls, management controls, operational controls, and procedures in order to provide layers of protection to the network infrastructure (Kamal, 2008; Hagen et al., 2008). Whitman and Mattord (2008) further explain that defense-in-depth provides redundancy throughout the network architecture by using technical controls. Firewalls are software and hardware that prevent unauthorized users from accessing the law firm network (Weaver, 2007). Anti-virus software scans files for potentially harmful viruses and sequesters these files to prevent their propagation (Lin, 2006) to other computers on the network. IDSs are software programs that identify possible unauthorized access to files (Basta & Halton, 2008). IPSs are software programs like IDSs that identify possible access to files but flag

the activity in real-time (Whitman & Mattord). Authorized users are those users who have permission to access the computer files and network of the law firm (Comerford, 2006). Access controls provide permissions to allow users access to network assets, such as database files or law firm networks based on their carefully delineated access privileges, making sure that only authorized users are allowed to access certain data on the law firm's network (Comerford).

Kamal (2008) further includes the use of information security policies, security awareness, and employee training to deflect social engineering schemes as other security layers to be included in the defense-in-depth process. Social engineering is the act of people attempting to coerce or trick someone into divulging secrets, such as their username and password to circumvent security protocols (Kamal; Basta & Halton, 2008; Medlin, Cazier, & Foulk, 2008). This can be accomplished by pretending to be an employee or someone knowledgeable (Kamal) about the law firm to gain the trust of the law firm employee in an attempt to retrieve sensitive information or bribing an employee to be unfaithful to the law firm (Basta & Halton).

Individuals who access law firm data without security measures in place may unknowingly put confidential information at risk (Salmela, 2008). Im and Baskerville (2005) found in their longitudinal study, as did Post and Kagan (2007) in their survey study, that human errors can be based on an individual's computer skill level. Errors can result in mistakes involving rules, or malfunctions of knowledge-based systems and can be intentional, accidental, malicious, direct attacks, or indirect attacks (D'Arcy & Hovav, 2009; Im & Baskerville; Kraemer & Carayon, 2007; Post & Kagan). LaRose, Rifon, and Enbody (2008) define self-efficacy as "the belief in one's own ability to carry out an

action in pursuit of a valued goal” (p. 72). In order to safeguard law firm data, an individual law firm employee has to believe that he/she is capable of making the proper security decisions (Chan, Woon, & Kankanhalli, 2005; LaRose et al.; West, 2008). Despite technical controls (i.e., firewalls, IDSs/IPSs, anti-virus, and access controls) that automatically assist in providing security measures, the provision of optimal security is challenging because humans are involved (Kraemer & Carayon; Post & Kagan; West). For example, a firewall can be misconfigured by a law firm employee resulting in a possible security breach or an e-mail attachment containing a virus can be opened without first scanning it causing a security breach incident (Comerford, 2006; Keller, Powell, Horstmann, Predmore, & Crawford, 2005). Security policies aid in defining how law firm employees should set up the firewall or when it is necessary to scan an attached file with anti-virus software prior to opening the file (Keller et al.; Verdon, 2006).

The design, implementation, and enforcement of security policies can be accomplished through a risk assessment such as an external or internal vulnerability assessment (Da Veiga & Eloff, 2007; Myler & Broadbent, 2006). An information security assessment typically consists of a risk assessment that identifies potential cyberthreats to a law firm’s mission critical resources and a vulnerability scan of applications, ports, and systems (Batista, 2006; Bowen et al., 2006). An information security risk assessment examines how law firm employees are actually following the information security policies and procedures (Bowen, et al.). A risk assessment can aid in determining the strength of the defense-in-depth of the multiple technologies installed to protect confidential and sensitive information residing on law firm networks (Batista). Typically, law firms perform an information security risk assessment to identify potential

threats, determine the likelihood (ranked high, medium, or low) that these threats will occur, and evaluate the impact (ranked high, medium, or low) on the law firm's functions should these threats transpire (Bowen et al.).

A vulnerability assessment consists of scanning the network and systems to identify exploitable vulnerabilities of the installed applications and to identify what patches and controls are needed to mitigate exposure of the confidential data to unauthorized users (Batista, 2006; Myler & Broadbent, 2006). Vulnerability assessments also scan the ports to identify whether there are exposed ports open that should be closed (Batista; Bowen et al., 2006) to prevent unauthorized users from gaining access to the law firm network infrastructure (Comerford, 2006). This vulnerability assessment can also aid in determining the effectiveness of law firm security policies and procedures (Batista; Bowen et al.; Ross, 2007).

Problem Statement and Goal

Problem Statement

With the proliferation of electronic documents in the legal world, the volume of documents held by law firms has increased significantly (Gorga & Halberstam, 2007). Document-intensive cases also contribute to the need to share data and other content of a client's case with roaming law firm users, the client, and/or with co-counsel for collaborative purposes (Gorga & Halberstam). A security breach can result in the risk of an intrusion into the law firm's sensitive information (Comerford, 2006; Kraemer & Carayan, 2007; Ries, 2007; Schwartz & Janger, 2007). For instance, the intruder could potentially gain access to attorney-client privileged documents that may contain proprietary information, trade secrets, shareholder information, PII, and/or other private

data that may be damaging to a law firm if it were to become public (Comerford; Johnson, 2008; Ries). Lawyers have an ethical obligation to protect confidential information from inadvertent disclosure, including data stored on law firm networks, as well as data accessed remotely (Comerford; Johnson). Such disclosure can contribute to a loss of confidence in a law firm (Schwartz & Janger) and/or liability from malpractice claims against lawyers and the firm. Therefore, the problem examined in this investigation was determining whether information security policies assist with preventing unauthorized parties from accessing this sensitive information.

The author further investigated the exploratory analysis study of Doherty and Fulford (2005) in this dissertation investigation to determine whether security policies aid in abating security breach incidents against law firm data and networks. The author advanced the 2005 study by identifying whether information security policies were developed in response to security breach incidents or whether concern for security breaches prompted the development and implementation of security policies. Thus, in this dissertation investigation, the author posited questions relative to whether security policies are proactively or reactively developed.

Goal

The goal of this dissertation investigation was to develop an analysis of the survey data to determine whether law firms are proactive in their security policy development or reactive to security breach incidents. In this dissertation investigation, the author also investigated whether law firms utilize risk assessments, network vulnerability scans, and/or penetration tests to validate the intended information security policies and ensure

the existence of adequate safeguards from attackers and/or prevention of unauthorized access to law firm confidential information (Myler & Broadbent, 2006).

Effective security practices by law firm personnel may be realized through the development, implementation, and enforcement of security policies. Information security policies outline the acceptable actions and uses of law firm computers and networks, and articulate procedures for secure access to the law firm's information resources (Da Veiga & Eloff, 2007; Doherty & Fulford, 2005; Kamal, 2008). Information security policies are identified as an integral part of information security best practices (Baker & Wallace, 2007; Da Veiga & Eloff; Doherty & Fulford; Hong, Chi, Chao, & Tang, 2006; Keller et al., 2005; Metzler, 2007; Myler & Broadbent, 2006; Verdon, 2006).

The likelihood that law firm employees will implement security measures is inversely proportional to the security measures' difficulty and/or complexity. For example, if law firm employees must download and install a software patch before opening a file, they may find it too time consuming and as a result find a way to by-pass performing this action in the future (LaRose, et al., 2008; Post & Kagan, 2007). Consequently, the complexity of computer safety measures may weaken security (Furnell, Jusoh, & Katsabas, 2006; LaRose et al.; West, 2008).

A practical example of this phenomenon can be seen in the use of computer passwords. A weak password is a password that can be easily guessed and typically consists of common words found in the dictionary (Basta & Halton, 2008; Beaver, 2007; Fordham, 2008; Garrison, 2008; Richardson, 2006). A password cracking software tool can quickly and easily discover a weak password (Garrison; Richardson). In contrast, a strong password consists of a combination of upper and lower case letters, numbers

and/or alphanumeric special characters (not at the end of the password). Additionally, the length of the password should be longer than eight characters and should not form a word in the dictionary (Basta & Halton; Harrison, 2006; Keller et al., 2005; Richardson). An example of a strong password that uses a combination of special characters, lower and upper case letters, and numbers is Nov@South3@\$t3rnUniv3r\$ity. However, if strong passwords become too difficult to remember, the law firm employees will write them down and carry them about or place it near the computer, thus resulting in weakened security (Comerford, 2006; Fordham; Keller et al.). Therefore, to be effective, security solutions must be perceived as practical and not unduly burdensome (Cannoy, Palvia, & Schilhavy, 2006; Fordham; LaRose et al.; Metzler, 2007; Post & Kagan, 2007). As a consequence, the perception of self-efficacy of security technologies was examined as well.

Relevance, Significance, and Need for the Study

Doherty and Fulford (2005) examined the role of information security policies in relation to the number and severity of security breaches. This survey was mailed to 2,838 information technology (IT) directors from large United Kingdom (U.K.) based organizations (employing more than 250 people) with 219 valid responses (7.7% response rate) returned. The majority of responses were received from those organizations employing fewer than 1,000 employees (44%) and between 1,000 and 5,000 employees (33%) with 23% of the respondents employing more than 5,000 employees (Doherty & Fulford). The survey instrument was validated by Doherty and Fulford through two pre-tests and a pilot study exercise distributed to experienced information security researchers and senior IT professionals with information security

duties (Doherty & Fulford). Doherty and Fulford found there was “no statistically significant relationship between the existence and application of information security policies and the incidence or severity of security breaches” (p.36). According to Doherty and Fulford, further research with different targeted samples was urgently needed.

The author included the original Doherty and Fulford (2005) survey instrument (N. Doherty, personal communication, January 13, 2007) in this dissertation investigation. Permission to use the Doherty and Fulford instrument in this dissertation investigation was received from Neil Doherty on January 13, 2007 with a confirmation of permission received again on December 8, 2008 (see Appendix A). Additionally, questions to determine the timing of security policy development in conjunction with security breach incidents have been developed by the author and reviewed by subject matter experts, Mark Thorogood, M.S., Ruth S. Stevens, M.L.S, J.D, and Anne K. Abatte, Ph.D. Surveying members of the legal community (Wiant, 2005) in this dissertation investigation facilitated the discovery of how this community, which is a different population from the Doherty and Fulford study, compared to the results from their 2005 study (Doherty & Fulford, 2005).

Wiant (2005) also recommended further research regarding the effect information security policies have on reducing the number of security breaches. Kraemer and Carayon (2007) urged additional research with regard to how security policies influence computer security and information security in organizations. Siponen and Oinas-Kukkonen (2007) recommended additional qualitative studies regarding high level information security policies from an organizational perspective.

With security breach incidents announced on a regular basis in the media (Conger, 2009), research regarding the impact of information security policies on reducing the number of security breaches is highly relevant. Security breach notification laws in 45 United States (U.S.) states (excluding Alabama, Kentucky, Mississippi, New Mexico, and South Dakota), and the District of Columbia, Virgin Islands, and Puerto Rico (Greenberg, 2009) mandate in the event of the compromise of personal data that clients be notified of the security breach incident (Heitzenrater, 2008; Johnson, 2008; Kugele & Placer, 2007; Schwartz & Janger, 2007; Silverman, 2007). Many of these laws define compromised PII as unencrypted customer information (Schwartz & Janger). PII is a combination of a person's first name or initial with last name, Social Security Number (SSN), driver's license number or state issued identification card, debit/credit card number with or without the security code, and/or medical information (Heitzenrater; Kugele & Placer; Silverman). Law firms collect some PII from their clients and also retain employee PII. In the event of a security breach wherein this information is exposed to or compromised by unauthorized parties, including insiders, the requisite notification procedures go into effect (Johnson; Kugele & Placer; Schwartz & Janger; Silverman).

On September 19, 2008, the Massachusetts Office of Consumer Affairs and Business Regulation issued a set of Code of Massachusetts Regulations (CMR), referred to as "201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth" which describes the expectations and requirements on how to safeguard residents' personal information in both paper and electronic formats (Massachusetts OCAB, 2008). These regulations were initially set to be effective on January 1, 2009. However, due to the overwhelming requirements contained therein, this date was delayed

initially to May 1, 2009, and most recently on November 4, 2009 delayed to March 1, 2010 (Lefferts, 2009). Law firms with clients who are residents of Massachusetts must comply with these regulations.

These security breach notification laws are similar to the California Senate Bill 1386 (SB 1386) (2002), the Gramm-Leach-Bliley Act (GLBA) (1999), the Health Insurance and Portability and Accountability Act (HIPAA) (CMS, 2003), and the Sarbanes-Oxley Act (SOX) (2002). On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act (ARRA) of 2009 which included a section entitled Health Information Technology for Economic and Clinical Health (HITECH) Act. Pursuant to the HITECH Act, there is now a federal security breach notification requirement for the healthcare industry requiring notification of a breach involving any type of personal information retained by a healthcare entity (Congress, 2009; Holloway & Fensholt, 2009). Law firms have clients who must comply with these regulations. When protected data are transferred to the law firm by the client, the law firm must also comply with the regulations and provide adequate safeguards (Comerford, 2006; Johnson, 2008; Ries, 2007). For example, if the law firm receives PII, such as electronic protected health information (ePHI) from a healthcare client, the law firm would become a business associate under HIPAA and must share in providing protections to the ePHI while it is in the law firm's possession (Li & Shaw, 2008; Swire & Bermann, 2007). Law firms also must abide by applicable state security breach notification laws with regard to their employee records in the event employees' SSNs or bank accounts, or other financial information is breached (Johnson; Kugele & Placer, 2007; Schwartz & Janger, 2007).

Barriers and Issues

Law firms consist of lawyers and members of their support staff, such as paralegals and legal secretaries (Hadfield, 2008) whose primary concern is the practice of law. In the legal profession, paralegals and lawyers generally have little, if any, formal training in the use of security applications, such as encryption or IDSs (Hadfield; Nelson et al., 2006; Ries, 2007). They may have little desire to engage in this type of training since their focus is on the practice of law. This lack of interest and training may result in reluctance to budget funds for IT staff, computer security risk and vulnerability assessments, and/or security products to ensure data security (Baker & Wallace, 2007). The lack of funds and management buy-in may result in a law firm having minimal IT personnel and, therefore, may not support security measures for its documents and/or databases and information resources (Nelson et al.).

According to Cannoy et al. (2006), typically organizations are unwilling to share security information with researchers. As a result, law firms may be reluctant to disclose their security breach incidents and security issues as well.

Roster, Rogers, Hozier, Baker, and Albaum (2007) state that having the survey e-mail link perceived as spam is a major potential barrier of online surveys. In an effort to combat this weakness, ILTA agreed to send out e-mail invitations with an introduction to the author and a link to the ILTA Website where ILTA members could preview a copy of the Zoomerang online survey in Portable Document Format (PDF) format prior to agreeing to participate in the survey. ILTA also included in the e-mail message, a link directing potential ILTA participants to the anonymous Web-based survey on Zoomerang.com. By providing a link to the survey on Zoomerang.com rather than

obtaining an e-mail list from ILTA to import into Zoomerang, the results of the survey were anonymous. Since ILTA members receive numerous survey requests from ILTA each year, they should have ILTA on their whitelist to prevent the e-mail from going into their spam e-mail.

Research Questions Investigated

The Web-based survey used in this dissertation investigation consisted of 10 primary research questions. The first five questions were derived from Doherty and Fulford's (2005) research on the relationship between written information security policies and security breaches in an exploratory analysis of U.K. organizations employing more than 250 people. The author converted their hypotheses into research questions for this Web-based survey in order to discover how law firms compare to the subjects in the Doherty and Fulford study. The additional five research questions were designed to investigate how information security policies impact law firms. The 10 primary questions investigated included:

1. Do law firms that have written information security policies have fewer security breach incidents in terms of frequency and severity than those that do not have information security policies (Doherty & Fulford, 2005, p. 25)?
2. Are law firms that have had information security policies in place for numerous years likely to have fewer computer security breach incidents in terms of both frequency and severity than those that do not have information security policies in place (Doherty & Fulford, 2005, p. 25)?
3. Do law firms that have updated their information security policies on a regular basis have fewer security breach incidents in terms of frequency and severity than

those that have not updated their information security policies (Doherty & Fulford, 2005, p. 26)?

4. Are law firms that have an information security policy with a broad scope likely to have fewer security breaches in terms of both frequency and severity than those organizations that do not (Doherty & Fulford, 2005, p. 26)?
5. Are law firms that have adopted a wide variety of best practices likely to have fewer security breaches in terms of both frequency and severity than those organizations that have not (Doherty & Fulford, 2005, p. 26)?
6. When under a time deadline to finish an assignment, are law firm employees more likely to by-pass security measures in order to complete the task (Post & Kagan, 2007)?
7. Are law firm security policies created in response to an information security breach incident (Doherty & Fulford, 2005; Wiant, 2005)?
8. Are risk assessments, network vulnerability scans, and/or penetration tests a part of law firms' validation of the intended security policies (Myler & Broadbent, 2006; Verdon, 2006)?
9. Do larger law firms (more than 251 users) and smaller law firms (less than 250 users) differ in whether they have written information security policies (Gibney & Corham, 2008)?
10. Do smaller law firms (less than 250 employees) and larger law firms (more than 251 users) differ in whether written information security policies were due to information security breach incidents (Gibney & Corham, 2008)?

Limitations and Delimitations of the Study

This investigation is limited to a select population of law firm IT professionals who are members of the International Legal Technology Association (ILTA). The author determined that ILTA would provide the most purposeful sampling available (Creswell & Clark, 2007; Patton, 2002). This study was limited by law firms who were ILTA members and by those who chose to answer the survey questions presented to them (Cannoy et al., 2006; Post & Kagan, 2007).

ILTA's 2008 Technology Survey defines the size of law firms by total number of users of the law firm's computers (Gibney & Corham, 2008). These law firm sizes are quantified as small (less than 151 users), medium (between 151-250 users), large (251-500 users) and very large (greater than 500 users) law firms (Gibney & Corham). Other measures of size of law firm may be number of lawyers rather than total number of users. Thus, this investigation was limited by the ILTA definition of law firm size as total number of users (Cannoy et al., 2006; Post & Kagan, 2007).

Small law firms with less than 150 employees may not dedicate resources to security or have information security policies as compared to large law firms of over 500 employees, who may invest more fully in security and security personnel (Doherty & Fulford, 2005). Thus, personnel in small law firms may not be aware of security breach incidents. External factors such as budgeting for security or security personnel may adversely impact the ability of smaller law firms to purchase and implement security technologies (Doherty & Fulford).

A vast body of international data privacy laws exists (Swire & Bermann, 2007). International law firms and law firms with global clients need to be cognizant of these

laws (Wugmeister, Retzer, & Rich, 2007). The delimitation of this research is that an exhaustive survey of global privacy laws was beyond the scope of this dissertation. However, an overview of some key international privacy laws was discussed in this dissertation.

Definition of Terms

The key terms utilized in this investigation are defined in this section. A list of acronyms is included in Appendix B.

Access control – Permission granted to authorize users to read and/or write to files on a computer or network through programs and information security policies (Whitman & Mattord, 2008).

Anti-spyware – Software detection program that alerts the computer user of software programs attempting to secretly collect confidential information from the computer user's files (Lin, 2006).

Anti-virus – Software that scans files to identify and quarantine harmful files that could compromise data (Siponen & Oinas-Kukkonen, 2007).

Authorized user – A person who has been granted read and/or write access to a computer or network (Comerford, 2006).

Confidential information – Personal data that may include PII, trade secrets, and financial, shareholder, or attorney-client privileged information (Comerford, 2006; Nelson et al., 2006; Ries, 2007).

Electronic Networks – Use of computer-based technology, such as a personal digital assistant (PDA), listserv, social networking Websites, blogs, and/or e-mail, to communicate with others (Taylor & Murthy, 2009).

Encryption – Software that uses mathematical algorithms to hide the content of a computer file or hard drive through the use of ciphertext (Stream & Fletcher, 2008).

Firewalls – Software or hardware that filters the traffic of the network to prevent unauthorized access (Siponen & Oinas-Kukkonen, 2007).

Human error – Mistakes or incorrect security decisions made by law firm personnel that expose the law firm computers and/or network to security breaches (Kraemer & Carayon, 2007).

Identity theft – Stealing the identifying credentials such as PII of another person to obtain credit cards for the monetary gain of the thief (FTC, 2007; Rey, 2008).

Information security policies – Written documentation outlining the structure of the law firm's security posture. Security policies outline the acceptable actions and uses of law firm computers and networks by their employees (Baker & Wallace, 2007; Da Veiga & Eloff, 2007; Doherty & Fulford, 2005; Metzler, 2007; Ries, 2007; Verdon, 2006).

Intrusion detection systems (IDSs) – Software programs that scan the perimeter of the network as well as the network to identify possible intruders to the computer systems and alert the user of this unauthorized access (Basta & Halton, 2008).

Intrusion prevention systems (IPSs) – Software programs similar to IDSs that include an additional feature of alerting the user in real-time of a possible unauthorized access attempt against the network or computer files (Whitman & Mattord, 2008).

Law firm size – Law firm size is measured by the number of employees using computers in a law firm (Gibney & Corham, 2008).

Management controls – Vulnerability assessments, security policies, and security plans, implemented to manage the security (Bowen et al., 2006) of the law firm’s computer systems and network.

Network vulnerability scans – Use of a variety of software tools to scan law firm computers and networks to identify whether software vulnerability patches are and if so, which ones, that may allow unauthorized persons to breach the security of law firm computers and networks (Batista, 2006).

Operational controls – Physical security, personnel security, business continuity planning, incident response, hardware and software maintenance, confidential data protection, and security awareness training (Bowen, et al., 2006) that are implemented by law firm personnel rather than automatically by computer software.

Penetration tests – Use of software tools to exploit vulnerabilities found in software applications (Bowen, et al., 2006) to gain access to law firm networks.

Personally identifiable information (PII) – Information that is unique to an individual and used to specifically identify a person (Kugele & Placer, 2007; Ries, 2007; Silverman, 2007). This information includes the combination of a person’s first name or initial with that person’s last name, and with any of the following: SSN, account number, driver’s license number, debit/credit card number, and/or medical information (Heitzenrater, 2008; Kugele & Placer; Silverman; Swire & Bermann, 2007).

Risk assessments –Examination of security policies and identification of potential security threats to a law firm’s mission critical resources through interviews of law firm personnel, as well as the use of a vulnerability scan of applications, ports, and systems (Batista, 2006; Bowen, et al., 2006; Ries, 2007).

Security breach incidents – Exposure of sensitive or confidential data, such as PII, trade secrets, intellectual properties, business processes, or other proprietary information to unauthorized persons (Doherty & Fulford, 2005; Heitzenrater, 2008; Schwartz & Janger, 2007; Wiant, 2005). These incidents can be accidental, intentional, malicious, or human error (Kraemer & Carayon, 2007).

Security controls – Software products for access control, anti-virus, anti-spyware, encryption, firewalls, IDSs and IPSs (Kamal, 2008; Whitman & Mattord, 2008) installed on law firm computers and networks.

Security measures – Incorporation of management controls, operational controls, and technical controls in an effort to safeguard data on law firm computers and networks (Bowen et al., 2006; Da Veiga & Eloff, 2007).

Self-efficacy – An individual's belief that he/she is capable of making the proper security decisions to safeguard data (Chan et al., 2005; D'Arcy & Hovav, 2009; LaRose et al., 2008).

Social engineering – Coercing, tricking, or manipulating behavioral changes of another person (Kamal, 2008; Medlin et al., 2008).

Technical controls – Security controls, such as access controls, audit logs, biometrics, and user authentication that assist with the detection of security violations by automated software programs (Bowen et al., 2006). Technical controls, such as anti-virus software, anti-spyware software, IDSs/IPSs, and data leakage content filtering, assist with enforcement of law firm security policies (Batista, 2006; Whitman & Mattord, 2008).

Threats – Anything with the potential to cause harm to the data residing on the law firm network or on any other computer device of the law firm (Comerford, 2006). There

are natural, human, and environmental threats (Bowen et al., 2006). Threats can include deliberate acts, physical attacks, remote penetration attacks, human errors, acts of God, technical control failures, operational issues, or social engineering wherein someone is tricked into divulging his/her username and password (Furnell et al., 2006; Kraemer & Carayon, 2007; Whitman & Mattord, 2008).

Vulnerability Assessments – Security assessments based on the use of software tools to determine whether the controls that a law firm has implemented have any security holes potentially enabling a user to gain access to data without authorization (Batista, 2006).

Summary

A large volume of highly confidential and sensitive information is stored on law firm computer hard drives and servers (Comerford, 2006). In the event that an unauthorized individual gains on-site or remote access to this equipment, the information could be compromised and the firm's reputation destroyed (Bisel, 2007; Comerford; Johnson, 2008). The financial losses associated with the disclosure of sensitive information can be staggering (Bisel). Ever increasing use of laptops and other portable media devices by the attorney workforce (Comerford; Gibney & Corham, 2008) raises the risk of inadvertent disclosure.

Doherty and Fulford (2005) performed an exploratory analysis of security policies and security breach incidents that highlighted the need for follow-up research with different target populations. This dissertation investigation advanced the research of Doherty and Fulford by targeting information security policies in law firms. Included in this dissertation investigation were Doherty and Fulford's original survey questions along

with additional questions posited to determine the timing of security policy development in conjunction with security breach incidents in a survey distributed by the author to ILTA members.

As clients continue to entrust their intellectual property, trade secrets, PII, and other proprietary material to their attorneys, law firms have a corresponding ethical obligation to safeguard this information from any type of security breach (Comerford, 2006; Johnson, 2008; Ries, 2007). Security policies and procedures specify what is expected of authorized users in protecting law firm database content and documents (Comerford). This dissertation investigation determined the effectiveness of law firm information security policies, implemented either proactively or reactively (Cannoy et al., 2006), in reducing the number of security breach incidents. The perception of self-efficacy of the use of security technologies by law firm employees as security measures was also discovered (Post & Kagan, 2007). Capabilities of risk assessments, network vulnerability scans, and/or penetration tests to validate the intended security policies and controls (Myler & Broadbent, 2006; Verdon, 2006) to assist with safeguarding law firm data were noted.

Chapter 2

Review of the Literature

Introduction

In this literature review, the author provides an analysis of the impact of information security policies on computer security breaches in law firms. Next, the author examines information security policies and computer security breach incidents in relation to safeguarding client data. Then, the author reviews topics relevant to security breach notification laws, U.S. and international privacy laws, data breach incidents, data leakage threats, and information security assessment procedures. The chapter concludes with what is known and unknown regarding this topic along with the contribution this study makes to the field.

The Theory and Research Literature Specific to the Topic

Security Policies

According to Baker and Wallace (2007), a security policy defines actions that can and cannot be taken with company computers. Security policies outline the acceptable actions and use of law firm computers and networks by law firm employees (Doherty & Fulford, 2005; Metzler, 2007; Verdon, 2006). Information security policies consist of written documentation outlining the structure of the organization's security posture. Typically, security policies provide guidance with regard to the physical and remote

access to data of the law firm. According to Doherty and Fulford (2006), information security policies should be in line with the law firm objectives.

Verdon (2006) found that “threats continually evolve, and the countermeasures must evolve too” (p. 47). After reviewing the potential threats to the law firm network, the law firm CSO (Chief Security Officer) and/or CIO (Chief Information Officer) should develop, implement, and distribute a security policy or policies to all employees.

According to Whitman and Mattord (2008) and Greene (2006) an effective security policy must establish key goals for ensuring that authorized users can access the network and information resources. Additionally, the security policy must ensure employees know the penalties of inappropriate behavior when using the law firm information resources and/or assets. Within the policy, each law firm employee’s information security responsibilities to protect the confidentiality, integrity, and availability of the law firm PII and confidential data (Whitman and Mattord; Greene) must be communicated.

Security policies are generally a snapshot in time (Belsis & Kokolakis, 2005). Thus, Metzler (2007) suggested using standards or security processes rather than just security policies to address the continual need to update the requirements as part of security policy maintenance. According to Metzler, organization stakeholders’ involvement is critical in order to produce longevity and effective security policies. In order to achieve these security goals, law firm managing partners and IT staff must be actively involved in developing these policies. If the security failure can be equated to a monetary figure, then the seriousness of developing an applicable security policy is more readily accepted by the managing partners (Greene, 2006; Nelson et al., 2006; Whitman & Mattord, 2008).

Security policies cover topics such as: acceptable use, access control, business continuity and disaster recovery, change control management, confidentiality, data classification, data backup and recovery, disposal practices, e-mail practices, encryption, information protection, information systems security, Internet use, network security, privacy, physical security, remote access, system administration security, incident response, and termination (Greene, 2006; Metzler, 2007; Rotvold, 2008; Verdon, 2006). All of these information security policies provide a legal defense in lawsuits and regulatory compliance (Nelson et al., 2006). Metzler suggests developing a separate security policy for each topic in order to quickly update and approve procedures. Therefore, smaller separate documents rather than one large document would expedite revisions and approval of necessary revisions to the individual topic policies since they would be shorter and therefore easier to review.

Incorporated in the security policy is a clear explanation of the rules with regard to how the network can be accessed, with a concentration on maintaining confidentiality and identifying the ramifications of a security breach (Greene, 2006; Whitman & Mattord, 2008). Distribution of the security policy to all law firm employees (Chen, Shaw, & Yang, 2006; Metzler, 2007) is of paramount importance. Security awareness is a topic all law firm employees must understand so their actions will not jeopardize confidential data in their possession (Nelson et al., 2006). Therefore, law firm employees must be informed as to the applicable security policy pertinent to their job and understand why it is important to protect the information located on their computers from unauthorized access (Baker & Wallace, 2007; Chen et al.; Metzler).

Insider threats consisting of the disgruntled or curious employee must be addressed in the security policies to outline the ramifications of accessing data not relevant to the law firm employee's job description (Gupta & Hammond, 2005; Lin, 2006). Insider threats are one of the most common causes of security breaches (Bowen et al., 2006; Chan, et al., 2005; Chen et al., 2006; Ramim & Levy, 2006). Incident response procedures and the method for reporting information security incidents relative to insider breaches should be included in law firm security policies (Chen et al.; Goldberg, 2008; Nelson et al., 2006).

Attendance at security policy awareness training sessions on information security incident reporting should be required of all law firm employees (Chen et al., 2006; Gupta & Hammond, 2005; Kim, 2005; Rotvold, 2008) on an annual basis. Rotvold suggests training attendance be a mandatory requirement incorporated into employee evaluations in order to assure enforcement of the security policy. Rotvold further found with regard to security policies that, "the top three personal motivators reported for compliance were individual motivation, followed by employee responsibility for information security, and importance placed on information security" (p. 37). Thus, communication of the seriousness of information security responsibilities by law firm management to law firm employees is critical in building a culture wherein it is second nature for employees to apply security measures (Rotvold).

Verdon (2006) underscores the importance of monitoring practices and the implementation of standards such as, ISO 27001:2005 (ISO/IEC 27001 Joint Technical Committee, 2005), National Institute of Standards and Technology (NIST), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), Control Objectives for Information and Related Technology (CoBIT) and Build Security In (a

Department of Homeland Security initiative). While other practices and standards are relevant to information security, the most recognized standard and controls are ISO/IEC 27001:2005 (ISO/IEC 27001 Joint Technical Committee) and ISO/IEC 27002:2005 (ISO/IEC 27002 Joint Technical Committee, 2005). The International Organization for Standardization (ISO) 27001:2005 *Information Technology – Security Techniques – Information Security Management Systems - Requirements* is an international security standard (ISO/IEC 27001 Joint Technical Committee) that specifies a framework of developing, establishing, utilizing, and maintaining an information security management system (ISMS). The relevant controls for ISO 27001:2005 that specify a framework of controls for structuring development of security policies (Humphreys, 2007; Myler & Broadbent, 2006) are described in detail in the ISO 27002:2005 *Information Technology – Security Techniques – Code of Practice for Information Security Management* (ISO/IEC 27002 Joint Technical Committee). These 12 controls include (1) risk assessment and treatment, (2) security policy, (3) organization of information security, (4) asset management, (5) human resources security, (6) physical and environmental security, (7) communications and operations management, (8) access control, (9) information systems acquisition, development and maintenance, (10) information security incident management, (11) business continuity management, and (12) compliance (ISO/IEC 27002 Joint Technical Committee). These specifications describe a framework for developing an ISMS and the controls required to implement administrative, operational, and management safeguards necessary to provide data protection and regulatory compliance (ISO/IEC 27001 Joint Technical Committee; ISO/IEC 27002 Joint Technical Committee). This international framework delineates a comprehensive outline

of what controls law firms should use to validate the effectiveness of their ISMS (Humphreys, 2007) protecting the client and law firm employee PII.

Siponen and Iivari (2006) examined six design theories focusing on when it would be acceptable for individuals to violate security policies for the good of the organization. While security policies are written for organizations as a whole, individuals are the ones who must abide by them. Exceptions are rare incidents of acceptable security policy violations (Siponen & Iivari; Verdon, 2006; Wugmeister et al., 2007). Wugmeister et al. point out that these exceptions outlined in the European Union (EU) Data Directive are only met:

. . . when one of the following exceptions is met: consent from the individual; contract necessity (that is, data may be used if necessary for the performance of the contract with the individual); compliance with (local) legal obligations; or the legitimate interests of the entity collecting the personal information outweigh the privacy interests of the individual (p. 456).

According to Siponen and Iivari, the EU has established data privacy directives predicated on an opt-in clause requiring an individual's permission prior to disclosing sensitive data. Each EU Member State is a country belonging to the EU (Swire & Bermann, 2007). Each of the Member States are encouraged to adopt their own privacy laws based on the European Commission Data Directive. Finland is an EU Member State with this opt-in requirement for permission from an individual prior to using his/her sensitive data (Wugmeister et al.). However, an acceptable exception to this clause was a Finnish tsunami victims'/survivors' Website which placed Finnish residents' names on it without consent since this action provided a higher level of service for the greater good of

the public (Siponen & Iivari). According to Verdon, exceptions should be included as an integral part of security policy development since they are valuable in demonstrating how employees should handle exceptions to achieve the greater good of the law firm.

U.S. Data Privacy Laws

In the U.S., state privacy laws require the review of security policies on an ongoing basis to ensure compliance with security breach notification requirements (Lin, 2006; Metzler, 2007; Verdon, 2006). There are security data breach notification laws in numerous states, as well as children protection laws and sections of federal laws protecting consumer's PII in finance and healthcare. Currently, no comprehensive federal data privacy laws in the U.S. directed specifically at law firms or private industries exist (Cassini, Medlin, & Romaniello, 2008; Jones, 2008; Otto, Antón, & Baumer, 2007). However, if law firms are entrusted with client information that contains PII from the client's customers, the law firm must protect this PII (Li & Shaw, 2008).

Several states recently passed specific data privacy laws (Worthen, 2008). Nevada passed Nevada Revised Statutes (NRS) 597.970, a data privacy law that went into effect on October 1, 2008 (Greenberg, 2008). This law mandates encryption for the transmission of Nevada customer PII through electronic means other than via a fax or on an internal secured system (Worthen). Massachusetts General Law (M.G.L.) 93H regarding security breach notifications became effective October 31, 2007. In conjunction with this law, on September 19, 2008, the Massachusetts Office of Consumer Affairs and Business Regulation issued a set of Regulations, referred to as "201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth" originally slated to go into effect on January 1, 2009, but now due to the

economic climate will go into effect on March 1, 2010 (Lefferts, 2009), regulating PII of Massachusetts residents, whether or not that business maintains a presence within Massachusetts (Worthen). The development of a written comprehensive information security plan that includes security policies and security breach notifications is outlined in this Massachusetts regulation (Massachusetts OCAB, 2009). Like all businesses, law firms must comply with this Massachusetts law by encrypting laptops and removable media devices containing PII, as well as encrypting e-mail messages containing PII. Thus, if the law firm collects credit card payments or SSNs from their Nevada or Massachusetts clients, they must comply with these laws.

Law firms must be cognizant of many laws that relate to their clients. A non-exhaustive sampling of some of the most significant laws and regulations that must be complied with in the U.S. are as follows:

Security Data Breach Notification Laws

A landmark security breach event occurred in 2005 when ChoicePoint, a data aggregator of PII headquartered in Georgia, announced it had unknowingly sold close to 145,000 people's PII to a criminal (Greenberg, 2008; Jones, 2008; Miller, 2007; Otto et al., 2007). The penalties for disclosing this PII were severe for ChoicePoint with penalties totaling \$15 million and an additional \$9 million in legal fees (Foley, 2008). With the ever increasing number of computerized PII records along with other data collected and subsequently retained by various organizations, including law firms, the odds of this data being compromised is high. As a result, in 2005, many states began to create data security breach notification laws similar to California Senate Bill (1386) of 2003 (Greenberg).

In the U.S. as of October 2009, 45 states as well as the District of Columbia, Puerto Rico, and the Virgin Islands have data security breach notification laws (Greenberg, 2009). Many of these laws define compromised PII as unencrypted customer information (Greenberg). PII is a combination of a person's first name or initial with last name, SSN, driver's license number, debit/credit card number, account number, and/or medical information (Kugele & Placer, 2007; Silverman, 2007). As depicted in Figure 1, the six states that did not have these types of laws as of December 2008 were Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota (Greenberg). Missouri added a data breach notification law in late July 2009 (Greenberg).

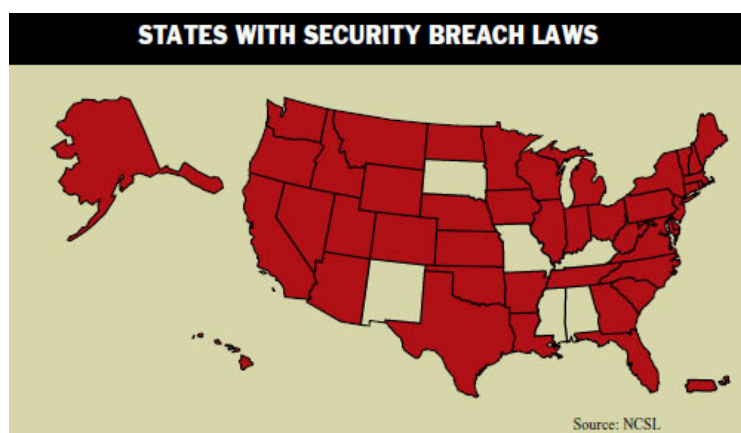


Figure 1. States with security breach laws map. Adapted with permission from ©National Conference of State Legislature (see Appendix A), “*Right to Know*,” by P. Greenberg, December 2008, p. 28, State Legislatures.

Overall, these laws mandate notification to state residents of lost, stolen, or compromised PII through unauthorized access to computerized data, including access by an unauthorized employee (Heitzenrater, 2008; Romanosky, Telang, & Acquisti, 2008). There is an overall exemption in every state data security breach notification law except for the state of Wyoming where reporting a security breach is not necessary if the compromised PII was encrypted (Greenberg, 2008). However, if the encryption key is

also compromised, this would then trigger the notification process. Many of the states also have a provision wherein if it can be determined that no reasonable harm will come of the compromised PII, then notification is not required (Romanosky et al.). A few states require that this determination be retained for three to five years.

Greenberg (2008) summarizes the 23 differences between the various state security breach notification laws. The variations outlined in Table 1 created by the author of this dissertation investigation includes eight states requiring specific details of the breach be included in the notice based on Greenberg's findings. Three states included paper in the definition of what constitutes a breach, along with five other states adding biometrics to their definitions of a data security breach incident (Greenberg). Health and medical information has been added to the PII definition of these states and Puerto Rico (Greenberg). Eight states and Puerto Rico require that the security breach incident also be reported to the Attorney General (Greenberg).

Table 1. Differences Within the State Security Breach Notification Laws

States	Exempt from Reporting if PII Encrypted	Includes Paper Breaches in Addition to Computerized Breaches	Broader PII Definition Including Medical or Health Insurance Information	Biometric Data if Released with Other PII	Specific Information about the Breach	Report to the Attorney General
Every state except Wyoming	X					
Alaska	X	X				
Arkansas	X		X			
California	X		X			
Hawaii	X	X			X	X
Iowa	X			X		
Maine	X					X
Maryland	X				X	
Massachusetts	X	X				X
Michigan	X		X		X	
Nebraska	X			X		

States	Exempt from Reporting if PII Encrypted	Includes Paper Breaches in Addition to Computerized Breaches	Broader PII Definition Including Medical or Health Insurance Information	Biometric Data if Released with Other PII	Specific Information about the Breach	Report to the Attorney General
New Hampshire	X				X	X
New Jersey	X					X
New York	X					X
North Carolina	X			X	X	X
Oregon	X				X	
Puerto Rico	X		X			X
South Carolina	X	X				
Texas	X			X		
Vermont	X				X	
Wisconsin	X			X		
Wyoming	X				X	
Virginia	X					X

Created from the data in the ©National Conference of State Legislature article, “*Right to Know*,” by P. Greenberg, December 2008, p. 27, State Legislatures.

These laws are pertinent to any business, including law firms, or an individual who collects PII, with an exemption for those entities who must comply with HIPAA or GLBA in some states (Hildebrand & Savare, 2008; Romanosky et al., 2008). Failure to notify those individuals whose PII are compromised carries a severe monetary penalty ranging from \$250 - \$500 per person to a maximum of \$750,000 per incident in some states (Schwartz & Janger, 2007). The critical distinction of these security breach notification laws is that notice is dependent upon where the consumer resides rather than where the business is located (Romanosky et al.). Notices to over 1,000 residents are permissible through mass media in most instances or if the cost of notification is over a specific monetary amount, such as \$5,000 in some states, up to more than \$250,000 in others (Silverman, 2007). Whenever the number of afflicted residents is more than 1,000

people, the majority of the state security breach notification laws require the company to notify the credit reporting agencies of the breach incident (Schwartz & Janger, 2007).

Romanosky et al. (2008) question whether the security breach notification laws actually affect the number of identity thefts. In Romanosky et al.'s study, they found "no statistically significant effect the laws reduce identity theft" (p. 1). However, Romanosky et al. also indicated that the data collected may be unreliable data gathered from Freedom of Information Act (FOIA) requests to the FTC. Moreover, data bias may exist as a consequence of inactivity by those individuals who personally knew the alleged identity thief (Romanosky et al.).

U.S. Identity Theft Regulations

Numerous risks are associated with unprotected PII. An identity theft risk involves how a law firm collects, uses, disseminates, and disposes of PII (Rey, 2008). News reports claim the exposure of numerous SSNs, credit card and debit card numbers, or medical information due to lost laptops, universal serial bus (USB) drives, or other portable media devices containing unencrypted PII (Bartlett & Smith, 2008; Berg, Freeman, & Schneider, 2008; Greenberg, 2008; Radcliff, 2008; Schreft, 2007). The use of e-mail to transmit PII without the use of encryption also provides an avenue for identity theft if this information is intercepted or sent to the incorrect e-mail address. Hacking into an unprotected computer is a method identity thieves use to procure unauthorized access to PII (Comerford, 2006; Johnson, 2008). Additionally, the physical thefts of credit card applications delivered through the mail or found in garbage by persons attempting to capture or steal someone's identity also place information integrity at risk. Improperly disposing of credit card applications, documents containing one's

SSN, medical records or pharmacy receipts in the garbage without first cross-strip shredding them also result in identity theft (FTC Business Alert, 2005).

The prevention of identity theft as a result of compromised PII and sensitive information in an organization's possession has been the focus of numerous laws in the U.S. as well as international laws. The Federal Trade Commission (FTC) describes the risk of identity theft as the loss of one's good credit that occurs when someone else steals an individual's identity and through the use of PII procures credit cards typically for cash advances as well as to make purchases of jewelry, electronics, or other items that can easily be converted into cash (FTC, 2007; Rey, 2008). Once the new credit card invoice is due, either one payment is made or no payments are made by identity thieves (FTC). As a consequence, the person whose identity has been stolen experiences deterioration in credit ratings and difficulties in procuring future credit (Rey).

FACTA (Fair and Accurate Credit Transaction Act) of 2003 was signed into law in 2003 to combat identity theft (Rey, 2008). In 2005, a disposal rule was created by the FTC, National Credit Union Administration (NCUA), and federal banking regulatory agencies requiring appropriate disposal of credit reporting information or information derived from credit reports (Federal Trade Commission, 2005; FTC Business Alert, 2005). The FACTA disposal rule requires that PII be burned, pulverized, or shredded (FTC Business Alert). This rule also describes the proper destruction of electronic media containing sensitive data to ensure that the information contained therein cannot be read, reconstructed, or used. The FTC Business Alert specifically indicated that attorneys must comply with the FACTA disposal rule.

The American Bar Association (ABA) challenged whether the FTC could assert that lawyers were considered financial institutions under the Gramm-Leach-Bliley Act if they provided financial services (Comerford, 2006; McMillion, 2006; Podgers, 2008). Title V of the GLBA (1999) focuses specifically on privacy and the protections of financial customer data (Cassini et al., 2008). Any non-public information in the possession of a financial institution must be protected from a security breach. Typically, GLBA supersedes other laws regarding data breach notifications (Greenberg, 2008). However, in the case of lawyers, they cannot be regulated by this financial institution law due to the 2005 U.S. Court of Appeals for the District of Columbia ruling in favor of the ABA that GLBA was not intended to regulate lawyers (Comerford, 2006; McMillion; Podgers). Thus, it is debatable whether the FTC can enforce the FACTA disposal rule with regard to law firms. Nonetheless, Comerford stated that FTC rules should still be used in a guidance role by law firms as a basis for ensuring good security practices when handling confidential client information.

Identity Theft Red Flags Rule

In 2005, the Federal Financial Institutions Examination Council (FFIEC) issued guidelines for safeguarding high risk transactions, such as online money transfers (FFIEC, 2005; Foley, 2008; Greene, 2006). According to the FFIEC, the confidentiality, integrity, availability, and non-repudiation of credit card information must be protected. FFIEC guidelines mandate development by financial institutions of a security program based on findings from a risk assessment (Foley; Greene; Nickell & Denyer, 2007); then implement the use of authentication appropriate for the level of risk (Cocheo, 2006; Hiltgen, Kramp, & Weigold, 2006). The Federal Deposit Insurance Corporation (FDIC)

issued guidelines to mitigate account-hijacking identity theft (FDIC, 2004) and defined additional multi-factor authentication procedures. These procedures include “something a person knows” such as shared secrets, out-of-band authentication (authenticated through a second medium, such as a cell phone, telephone, fax, or e-mail message), and challenge questions verification techniques (FDIC). Other options include the use of “something a person has” such as tokens and non-hardware based one-time password scratch cards (FDIC). Moreover, additional items under this category include Internet Protocol (IP) address location (match a previously used IP address), device authentication (authenticates the computer), geo-location (calculates location), and mutual authentication (digital certificate) (FDIC). Biometric identifiers such as fingerprints and retinal scans that verify “something a person is” are also increasingly employed (Cocheo; FDIC, 2005; FFIEC; Greene). According to Comerford (2006) these techniques would also be useful for attorneys safeguarding client data.

Stringent laws dealing with preparation of red flags to warn of identity theft were promulgated by the FTC in cooperation with five other U.S. regulatory agencies in 2008 (Rey, 2008). As an example, on January 1, 2008, the Office of the Comptroller of the Currency (OCC), Federal Reserve System (Board), FTC, FFIEC, FDIC, and National Credit Union Association (NCUA) endorsed the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003 Final Rule which became effective (FTC, 2007; Wernick, 2009). Federal Register Subpart J of the Red Flags Rule requires a risk assessment of identity theft protection plans and programs. Subpart J further outlines 26 practices and patterns that should raise red flags that identity theft may occur (FTC; Rey). The Red Flags include identifying suspicious PII, such as

address discrepancies, forged documents, improper use of SSNs from deceased persons, or unusual activity (FTC; Rey).

A mandatory Red Flags Rule compliance date of November 1, 2008 for all financial institutions was endorsed as well (FTC, 2007). However, many non-banking creditors, such as car dealerships and others who defer payment for goods or services did not realize that they too needed to comply with the Red Flags Rule. As a result, the FTC granted an extension to June 1, 2009 to these non-financial institution creditors and state-chartered credit unions to develop and implement their written identity theft prevention programs (Moscaritolo, 2009; Podgers, 2009). Despite the reprieve on the mandatory compliance date, the liabilities for failure to comply with the Red Flags Rule were activated. The penalty for non-compliance includes civil monetary penalties and remediation costs, and may result in loss of customers (Rey, 2008). The ABA filed a lawsuit opposing the FTC's claim that attorneys have to comply with these rules. The ABA's stance was that since attorneys ethically cannot bill for services until they have been rendered, this does not constitute a deferment of payment (Podgers). The case was decided by the U.S. District Court for the District of Columbia judge in favor of the ABA (Honorable R.B. Walton, 2009). However, the FTC has 30 days to appeal this ruling.

Currently, guidelines that specifically address law firm security like those for the financial industry are not yet available (M. Thorogood, personal communication, December 18, 2008). Nonetheless, law firms with financial institution clients are required by these clients to produce evidence of security safeguards for banking information entrusted to the law firm during litigation (Comerford, 2006).

PCI DSS (PCI Data Security Standards)

The Payment Card Industry Data Security Standards (PCI DSS) outline the security measures that must be implemented with regard to credit card information. These standards are required for safeguarding all credit card purchases (PCI Security Standards Council, 2008). Pursuant to PCI DSS, it is required that law firms not store any more cardholder data than is necessary, not store sensitive authentication data subsequent to authorization (even if encrypted), and mask the PAN (primary account number) when displayed (Berg et al, 2008). The first six and last four digits are the maximum number of digits to be displayed (Berg et al.). Law firms generally accept credit card payments for their services and must comply with the PCI DSS.

Health Insurance Portability and Accountability Act (HIPAA) of 1996

The enactment of the HIPAA of 1996 imposes restrictions on healthcare providers to ensure that patient medical records remain confidential, private, and secure (Greene, 2006; Kahn & Sheshadri, 2008; Li & Shaw, 2008; Wiant, 2005). HIPAA requires that remote access to any medical records have proper security safeguards in place (Baker & Wallace, 2007; Kahn & Sheshadri; Wiant). The HIPAA Security Rule dated February 20, 2003 requires that all ePHI whether at rest or transferred electronically, be encrypted and protected from interception by unauthorized parties (CMS, 2003; Li & Shaw). Covered entities include health care providers, healthcare plans, and clearinghouses (Holloway & Fensholt, 2009).

HIPAA imposes restrictions on healthcare providers to ensure that patient medical records remain confidential, private, and secure through the use of administrative, physical, and technical safeguards (CMS, 2003; Johnston & Warkentin, 2008). Protected

health information (PHI) can include paper documents, verbal communications, and electronic communications, such as electronic health records (EHRs), with only the electronic format of ePHI requiring administrative, physical, and technical safeguards (Cassini et al., 2008; Kahn & Sheshadri, 2008; Medlin et al., 2008). Patient name with medical diagnosis, laboratory results, medical history, SSNs, credit card numbers, names of doctors, and contact information are considered ePHI (Li & Shaw, 2008; Medlin et al.).

While the HIPAA Final Ruling does not require specific security measures (technology neutral), it provides guidelines with regard to what is reasonable and appropriate. The HIPAA Security Rule consists of 18 standards, which include 42 implementation specifications (CMS, 2003). Of the 42 implementation specifications, 20 are required specifications and 22 are addressable specifications. While a number of these requirements are listed as addressable, it does not mean they are optional. Rather, addressable means that if the risk assessment indicates they are necessary then these specifications should be addressed (CMS, 2003).

Covered entities must comply with the HIPAA Security Standards with respect to ePHI (Nahra, 2008). Covered entities are required to review, modify, and/or develop security measures that will provide reasonable and appropriate protection of ePHI by ensuring the confidentiality, integrity, and availability of the ePHI that is captured, maintained, and/or transmitted (Li & Shaw, 2008). Additionally, ePHI must be protected against reasonably anticipated threats, hazards, and unauthorized disclosures and security policies must be updated on an annual basis (Kahn & Sheshadri, 2008; Nahra). Anyone associated with the primary healthcare provider as a third party provider of services is

considered a Business Associate and also must comply with the HIPAA security provisions (CMS, 2003; Li & Shaw). For example, if the law firm receives patient identifiable information, such as ePHI from a healthcare client, the law firm would become a business associate under HIPAA and must share in providing protections to the ePHI while it is in their possession (Li & Shaw). The penalties for disclosure to unauthorized parties are substantial and can ruin the reputation of the law firm (Bisel, 2007).

The HITECH Act portion of the ARRA (Congress, 2009) requires that any unauthorized access to PHI must be reported to the affected individual within 60 days of the security breach discovery (Holloway & Fensholt, 2009). The 60 day time period begins upon the discovery of the unauthorized access by anyone in the organization (Congress). The notice requirements include an explanation of what happened, date of breach, what PHI was accessed, and the security countermeasures taken to mitigate the breach (Holloway & Fensholt). The HITECH Act also outlines new penalties depending on the circumstances of the breach as \$100 per violation up to \$1.5 million associated with HIPAA privacy and security breaches (Holloway & Fensholt).

International Data Privacy Laws

Historically, privacy laws started with the U.S. Privacy Act of 1974. The OECD (Organization for Economic Cooperation and Development) Privacy Principles were created in 1980 (Gunasekara, 2007). The content was developed by 23 countries, including the U.S., and provided guidelines for protecting, limiting, and securing the collected PII of individuals (Swire & Bermann, 2007). ISO/IEC 27001:2005 and ISO/IEC 27002:2005 are based on the OECD Privacy Principles (Humphreys, 2007). The

Asia Pacific Economic Cooperation (APEC) Privacy Principals are explicit data privacy laws (Swire & Bermann). According to Wugmeister et al. (2007), the APEC Privacy Principals incorporate OECD privacy principles of “notice, choice, collection limitation, use of personal information, data integrity, security safeguards, access and correction, and accountability” (p. 483). Wugmeister et al. further state that the APEC Privacy Principal expectations go above and beyond the OECD Privacy Principles by requiring the ethical handling of any and all PII when PII is being transferred even those items that are not necessarily required to be protected.

While the U.S. is an opt-out society, meaning personal data can be used until the person requests his/her data not be used, many other countries, including those in the EU are opt-in societies wherein the person’s consent is required prior to use of PII for any purpose (Swire & Bermann, 2007). In the EU countries, Canada, Australia, and Japan, data privacy is taken quite seriously. By way of example, the following is an overview of some key international privacy laws.

European Union (EU) Privacy Laws

The EU has explicit data privacy laws that are all encompassing with regard to vigorously protecting sensitive personal data (Swire & Bermann, 2007). Pursuant to the European Commission’s Directive, the EU definition regarding personal data refers to anything that can identify an individual and harm their dignity (Cassini et al., 2008). No sensitive data regarding any EU resident can be disseminated without written consent from the individual (Swire & Bermann). Employee data are classified as the most sensitive data that must be protected pursuant to the EU Data Directive. Data include business address, business phone number, title, sexual orientation, date of birth, trade

union membership, political opinions, national identification or social security number, credit/debit/charge card number, PIN, and photograph (Swire & Bermann). Employment applications, performance evaluations, drug tests, and terminations are also considered sensitive data. No PII or other sensitive data about an EU resident can be transferred to the U.S. without express written consent (Wugmeister et al., 2007). Law firms with global offices must be aware of the individual laws for each state belonging to the EU and how each EU state's laws relate to a data security breach of the law firm satellite office or offices located in that EU state (Goldberg, 2008). Raether (2008) further indicated if a breach of information from the European Economic Area of Iceland, Norway, and Liechtenstein occurs, that these laws would also pertain to law firms in these areas as well (Wugmeister et al.).

Canadian Privacy Laws

Canada also takes the privacy of their citizens very seriously. The Personal Information Protection and Electronic Documents Act (PIPEDA) of 1998 covers all industries and protects the collection, usage, and disclosure of personal information (Wugmeister et al., 2007). Similar to the European Directive, this law mandates a person's consent to allow his/her personal information to be used in any fashion, barring criminal investigations (Swire & Bermann, 2007). PIPEDA is based on the OECD Privacy Principles of accountability, purpose, consent, collection limitations, usage, disclosure and retention limitations, accuracy, safeguards, openness, individual access, and challenging compliance (Wugmeister et al.). The burden is on the collector to protect the PII collected and retained to ensure that the data is used only for the purpose it was collected (Gunasekara, 2007).

Safe Harbor

The EU and Canada have strict laws controlling third party transfers of data (Wugmeister et al., 2007). Thus, data cannot be removed from European countries or Canada without complying with many stringent standards. A law firm with satellite offices in European countries must obtain Safe Harbor certification prior to transferring any private data to their offices in any other country, including the U.S. (Wugmeister et al.). Safe Harbor certification is a laborious and expensive process (U. S. Department of Commerce, 2000). However, it aids with being able to send law firm paycheck information as well as transmittal of other sensitive information back to the U.S. Supplier contact databases, contract information and third party access to sensitive data, as well as customer databases and contract information, are all forms of personal information in Europe and must be protected (Swire & Bermann, 2007). Consequently, if the law firm's EU satellite office wants to exchange this type of information with their U.S. office, they must become Safe Harbor certified (Wugmeister et al.).

Data Leakage Threats

Whitman and Mattord (2008) classify threats as accidental, deliberate acts, physical attacks, remote penetration attacks, human errors, acts of God, technical control failures, operational issues, or social engineering wherein someone is tricked into divulging his/her username and password. Environmental, natural, and human threats (Bowen et al., 2006) to law firm data adversely impact a law firm's operations. Environmental threats include inadequate temperatures in law firm server closets, fires, and power outages (Bowen et al.; Nelson et al., 2006). Natural threats to law firms include hurricanes, floods, high winds, blizzards, tornadoes, earthquakes, volcanic explosions,

and wild fires (Myler & Broadbent, 2006). Environmental and natural threats also adversely impact the availability of law firm data. By contrast, a security breach results from lost, stolen, or compromised PII or confidential data through unauthorized access to computerized data (Cassini et al., 2008). Human threats, however, whether accidental or intentional (Whitman & Mattord, 2008) can directly compromise PII by facilitating unauthorized access to computerized data (Cassini, et al.).

Insider Threats

According to Comerford (2006) data at rest are even more at risk than e-mail messages in transit. Unencrypted data on servers and hard drives are at risk to unauthorized retrieval by employees and/or hackers (Gupta & Hammond, 2005; Wiant, 2005). The weakest factor in protecting PII and sensitive data from unauthorized disclosure is the insider (Bowen et al., 2006; D'Arcy & Hovav, 2009) who works for the law firm as an employee, attorney, or contractor. The consequences of losing a laptop or PDA containing sensitive law firm data or PII could lead to financial ruin in the form of a malpractice case resulting in bankruptcy and/or damage to a law firm's reputation (Comerford; Desouza, 2008). Additionally, removable media devices used by law firm employees may introduce a virus and/or malicious code into the network or individual computer while by-passing the IDSs and/or virus protection safeguards (Heikkila, 2007; Radcliff, 2008). These removable media devices also provide the capability to download gigabits of attorney-client privileged documents, work product information, and/or client data. Exposing law firm sensitive information and/or PII to unauthorized people poses a serious liability to the law firm (Goldberg, 2008).

Downloading and/or uploading pictures and software programs onto law firm networks without regard to the acceptable use security policy requiring an anti-virus scan of pictures and software prior to installation could result in a security breach or incident (Greene, 2006). In the absence of distributed written security policies outlining what can or cannot be downloaded, in conjunction with a lack of appropriate controls in place to prohibit unauthorized downloads from the Internet, there is a higher probability of law firm employees unknowingly compromising law firm computers (Metzler, 2007; Verdon, 2006). West (2008) states that users are unmotivated to download security software while in the middle of a project or they feel incapable of making an appropriate decision with regard to whether or not they should install security software. LaRose et al. (2008) found that fear inhibits user's self-efficacy regarding using security measures such as anti-spyware and the downloading of security patches. LaRose et al. further found that those who believed they were personally responsible for their computer's security were more inclined to take appropriate security actions as necessary.

Many of the security techniques for law firm users rely upon passwords to authenticate the user prior to gaining access to protected sensitive data on the law firm computers/networks (Basta & Halton, 2008). Employee usernames and passwords are utilized to access the network and files (Fordham, 2008) on the law firm servers. Although password files are often encrypted in ciphertext when stored on the server, the individual is the weakest link with regard to protecting the identity of the password (Bowen et al., 2006; Goldberg, 2008; Stream & Fletcher, 2008). According to Garrison (2008), passwords are quickly divulged to others within the corporation and sometimes to complete strangers outside of the organization, or they are taped to computer screens for

anyone with physical access to the computer to discover (Basta & Halton; Fordham; Goldberg; Metzler, 2007; Stream & Fletcher). Medlin et al. (2008) found that hospital employees who changed their passwords more often or had longer passwords were more willing to share those passwords through social engineering techniques such as entering a drawing to win a prize for giving up their password. Medlin et al. further stated that those hospital employees who had training were more likely to have strong passwords than their peers but still were willing to share them with internal hospital employees.

Passwords that are common words found in the dictionary make them susceptible to a dictionary attack or easily guessed because they relate to the immediate life of the password holder (Basta & Halton, 2008; Beaver, 2007; Fordham, 2008; Garrison, 2008). Fordham suggests using the first or second letters of the words in sentences that are easy to remember. For example, the sentence “Nova Southeastern University is a great institution to get your PhD” would translate to the strong password NSUi@gi2gyP.

Password mismanagement is another insider threat. The use of a default password is a high level threat since default password schemes are widely know by law firm employees and therefore trivial to guess (Beaver, 2007). Software default passwords may also readily be available on the Internet or through the software company Website (Beaver). Furthermore, if law firm employees are unaware of approaches for password protection, the likelihood of using default passwords increases (Gupta & Hammond, 2005; Metzler, 2007). In the event the default password naming scheme is widely known, curious and/or malicious individuals can readily access documents and e-mail accounts.

Additionally, the threat of compromised passwords increases with the hiring of contract attorneys (Gorga & Halberstam, 2007). With contract attorneys working on a

temporary basis, a large turnover of employees coupled with the ability to download large amounts of sensitive information onto USB flash drives (Heikkila, 2007) would provide the motive and resources to carry out a threat action (Radcliff, 2008). Temporary employees, who may not be invested in the law firm, may be able to access highly confidential information (Gorga & Halberstam), thereby placing the law firm PII and confidential information at risk. By surreptitiously logging in as an authorized user or contract attorney, these actions may disrupt network operations and his/her actions may not be traced (Heikkila, 2006). This is a high risk threat that must be addressed and controls put into place to protect against it. In the event that an intruder physically broke into the building, having data available without any type of password protection or encryption is an additional liability the law firm must also protect against (Comerford, 2006).

Another insider threat can originate within the IT Department. The sharing of one administrator username and password by the entire IT Department for accessing every network server is categorized as a high threat level practice (ISO/IEC 27002 Joint Technical Committee, 2005). An audit trail using automated monitoring software should be enforced (ISO/IEC 27002 Joint Technical Committee). However, when everyone shares the same administrative username and password, there is no audit trail to discover who made specific changes (ISO/IEC 27002 Joint Technical Committee; Kent & Souppaya, 2006). Aside from the login username and password for logging into the network, each member of a law firm IT Department should be assigned a unique username and password for the domain controller accounts (Kent & Souppaya). Use of the null default passwords poses a high threat level practice that can result in the

compromise of confidentiality, integrity, and availability of the network should a disgruntled employee or other unauthorized users initiate changes to the network servers (Wiant, 2005). Thus, individual administrator passwords for each IT Department employee should be changed on a regular basis, as should law firm employee passwords (Fordham, 2008).

Data Breach Incidents

How the law firm collects, uses, distributes, and disposes of both client and employee PII is impacted by identity theft risks associated with unsecured PII on law firm computer equipment or networks. There are a number of Websites that report data breaches with different sets of data security breach incidents reported to each. These Websites include government, medical, education and business in their sector categories with a few segregating banking/financial from the business category. The following are a composite of the 2008 breaches.

Pursuant to data compiled by Attrition.org, Etiolated.org, and the Open Security Foundation, as of December 31, 2008, there were 386 data breach incidents (Open Security Foundation, 2008). Figure 2 depicts these 386 data breach incidents by sector.

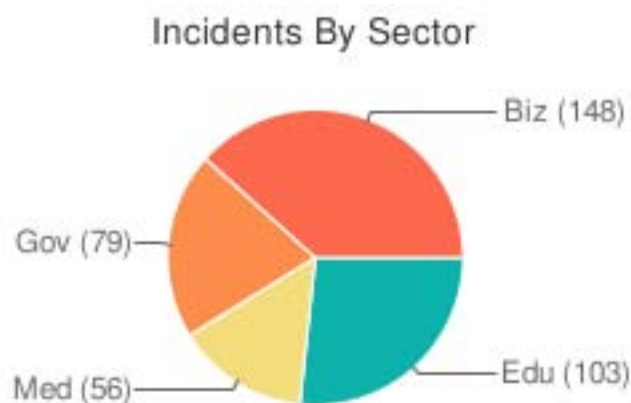


Figure 2. Incidents by sector. Adapted with permission courtesy DataLossDB.org, ©2008, Open Security Foundation (see Appendix A).

As depicted in Figure 2, Biz (business) lead all sectors in 2008 with 148 reported data security breaches. Edu (education) had 103 incidents, while Gov (government) reported 79 and Med (medical) 56 incidents. These reported security breaches comprised a number of different data types. Figure 3 shows the December 31, 2008 breakdown of these incidents by data type.

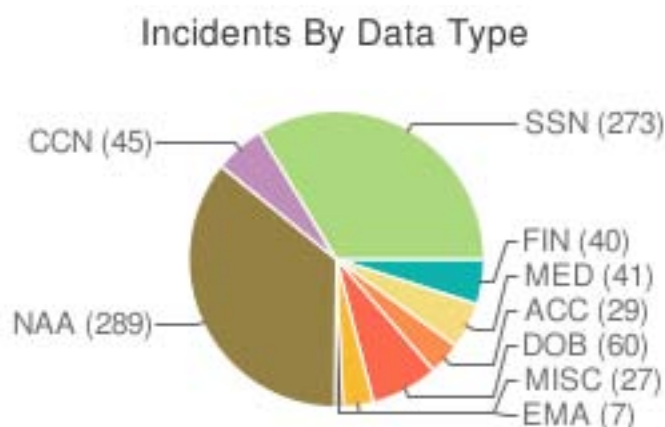


Figure 3. Incidents by data type. Adapted with permission courtesy DataLossDB.org, ©2008, Open Security Foundation (see Appendix A).

As depicted in Figure 3, NAA (names and addresses) were the data type most compromised with 289 incidents reported followed by 273 incidents of SSN breaches. The rest of the data types were substantially less in total numbers of incidents with 60 DOB (date of birth), 45 CCN (credit card numbers), 41 MED, 40 FIN (financial), 29 ACC (account information – financial), 27 MISC (miscellaneous), and 7 EMA (e-mail address) for 2008 (Open Security Foundation). Each data breach incident included a combination of data types that were compromised. SSNs are typically more valuable PII to identity thieves than names and addresses (Greene, 2006). However, in order to commit identity theft, the SSN in combination of the person’s name is necessary (Greene).

Open Security Foundation (2008) has been collecting security breach information since 2000. There were only a handful of security breaches reported during the early 2000's (Open Security Foundation). Once the ChoicePoint data breach occurred in 2005, there were 22 states that enacted security breach notification laws (Greenberg, 2008) and consequently there were significantly more security breach incidents reported (Otto et al., 2007). In 2005, 128 data breaches were reported (Open Security Foundation). Figure 4 shows the breakdown of types of breaches from 2000 through 2008 with laptops (21%) and hacking (20%) leading the types of all time breaches reported.

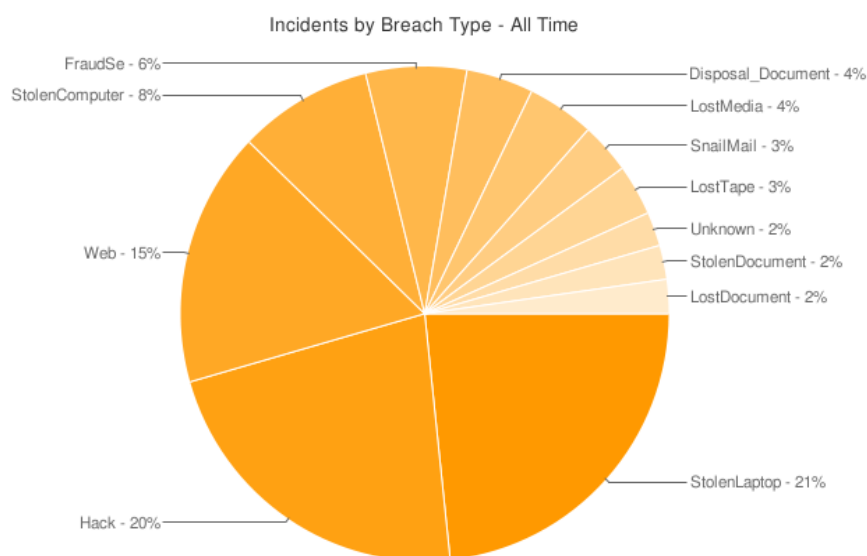


Figure 4: Incidents by Breach Type – All Time. Adapted with permission courtesy DataLossDB.org, ©2008, Open Security Foundation (see Appendix A).

On a yearly basis, the Identity Theft Resource Center (ITRC) also compiles a list of security breaches. ITRC has been collecting information for the past four years (Curtin & Ayres, 2009). Bartlett and Smith (2008) report exposure of PII as a risk management threat has been growing exponentially since 2006, up 140% from 2006 to 2007 with 448 data breaches. However, by August 2008, a record number of data breaches (449 compared to a total of 448 for all of 2007) had already been reported on the ITRC (ITRC,

2008a) breach list. As of December 31, 2008 for the year 2008, 656 data breaches and 35.6 million record exposures were reported to ITRC (2008b). This large increase of 47% over 2007 is attributed to underreporting in previous years and more than one organization reporting the same breach (ITRC, 2009).

For the year 2008, businesses lead the way on the ITRC list with 36.6% of the breaches followed by education, government/military, medical/healthcare, and banking (ITRC, 2008b). The banking industry, however, has more than half of the records that were compromised at 52.5% (ITRC, 2008b). A summary of the breakdown of the 2008 breaches outlined in the ITRC (2008b) data breach stats as of December 31, 2008 created by the author of this dissertation investigation depicted in Table 2 shows business as the leader in number of breaches with 240 breaches. However, banking exposed three times as many records than business in 2008 with 18.7 million records compromised.

Table 2. Summary of 656 Data Breaches

CATEGORY	# OF BREACHES	% OF BREACHES	# OF RECORDS	PERCENTAGE OF RECORDS
Banking	78	11.9%	18.7 M	52.5%
Business	240	36.6%	5.8 M	16.5%
Educational	131	20.0%	.80 M	2.3%
Government/Military	110	16.8%	2.9 M	8.3%
Medical/Healthcare	97	14.8%	7.3 M	20.5%

Created from the data in the ITRC 2008 Data Breach Stats (ITRC, 2008b).

The ITRC (2009) points out that government previously had the highest number of breaches in 2006 with 30% of the breaches but had substantially reduced that number to only 16.8% in 2008. According to ITRC (2009), “only 2.4% of all breaches had encryption or other strong protection methods in use. Only 8.5% of reported breaches had password protection” (p. 1). The ITRC 2008 data breach list shows only two Texas law firms and one Florida law firm as having reported a data breach (ITRC, 2008b).

One of the Texas law firms reporting a breach listed 672 records as being compromised. The other two law firms did not disclose the number of records breached (ITRC, 2008b). According to Curtin and Ayres (2009) in their analysis of the ITRC 2005, 2006, 2007, and 2008 reported data breaches, lost or stolen computing hardware were the largest contributors to breaches (29.14%), while insiders of an organization were responsible for 35% of the ITRC reported data breaches.

The Privacy Rights Clearinghouse collects security breach incident information from a number of sources, but their primary source is the Open Security Foundation Data Loss Database (Privacy Rights Clearinghouse, 2008). Their chronology of data breaches indicates there have been over 246 million breaches since 2005 (Privacy Rights Clearinghouse). Greenberg (2008) depicts in Figure 5 a 2008 breakdown of the 880 Privacy Rights Clearinghouse reported data breach notifications.

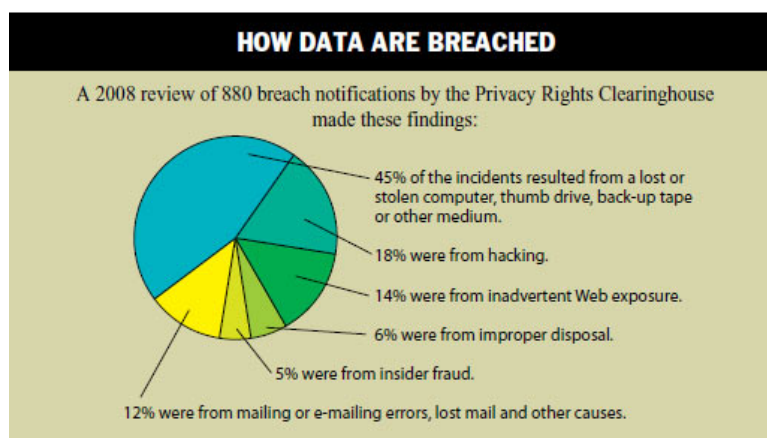


Figure 5. How data are breached. Adapted with permission from ©National Conference of State Legislature (see Appendix A), “*Right to Know*,” by P. Greenberg, December 2008, p. 27, State Legislatures.

The majority of the breaches (45%) were attributed to lost or stolen equipment, while hacking only contributed to 18% of these incidents. Inadvertent Web exposure (14%), lost mail (12%), improper disposal (6%), and insider fraud (5%) were the other reasons

provided for the incidents reported to the Privacy Rights Clearinghouse (Greenberg). Schwartz and Janger (2007) believe insider fraud reporting has historically been extremely low due to the fact that companies do not typically report insider abuse.

Romanosky et al. (2008) state there may be reporting biases with regard to who reports a data breach. According to Sveen, Sarriegi, Rich, and Gonzalez (2007) data breaches are typically under reported by employees due to disincentives such as embarrassment, lack of positive gains, fear of punitive measures or reprimands, and time allotment being too high for completion of reporting forms. In law firms, the lack of commitment and/or incentives to report a security breach incident can have serious consequences, such as malpractice and regulatory compliance penalties (Goldberg, 2008).

In 2007, TJX Companies, Inc., the parent company of a number of discount retailers, reported a large security breach involving 94 million Visa and Master Card records due to the inappropriate use of WEP (wired equivalent privacy) wireless security, inadequate storage of these records, and a failure to encrypt data at rest (Bartlett & Smith, 2008; Berg et al., 2008; Chandler, 2007; Heitzenrater, 2008). Due to the inadequate security solutions in place, hackers were able to break into the TJX Companies network and compromise these 94 million records for 18 months before being discovered. This data security breach crossed many jurisdictions (Chandler) and cost approximately \$4.5 billion (Berg et al.).

Another security breach incident reported in 2008 involved the Hannaford Brothers Supermarket chain (Bartlett & Smith, 2008). Approximately 4.2 million records were compromised by hackers (Bartlett & Smith). As noted by Swartz (2008) the numbers of records compromised typically are grossly understated. According to Bartlett and Smith

only a small percentage of compromised records are used in an illegal way. Despite the lack of criminal activity involved with compromised data, the trust of the client in the law firm that has reported a security breach incident may be damaged (Bartlett & Smith). However, Chandler (2007) stated that as large numbers of security breach notices are distributed, affected individuals become increasingly desensitized to these notifications.

Information Security Assessment

An information security assessment is a critical exercise for protecting the confidential and sensitive data (Humphreys, 2007; Salmela, 2008) that resides on a law firm's network and portable media devices (Batista, 2006; Heikkila, 2006). A security assessment based on a combination of a risk assessment that identifies the potential threats to mission critical assets of a law firm, along with vulnerability scans of applications, ports, and operating systems, including mission critical databases, assist in the mitigation and remediation of potential threats (Batista). Based on the identification of the mission critical assets that need the utmost protection and the level of risk accepted by law firm management, the scope of the vulnerability assessment is defined (Humphreys; Salmela). Natural, human, and environmental threats that are identified can aid in determining the management, operational, and technical controls implemented to remediate these threats (Bowen et al., 2006; Heikkila).

IT risk assessments are performed to protect vital business processes and key assets of a law firm (Batista, 2006; Salmela, 2008). According to Humphreys (2007), the goal of a risk assessment is to evaluate the impact of a threat based upon the confidentiality, integrity, and availability (CIA) approach in law firm environments (Batista). If a database becomes unavailable, the lawyers sit idle unable to bill time and as a

consequence thousands of dollars in revenue can be lost (Bisel, 2007). In the event that a database becomes corrupt or sensitive information is inadvertently disclosed, the cost can range from losing the case to losing the confidence of the client (Comerford, 2006; Desouza, 2008). The firm's reputation is at stake should the trust the client places in the law firm suddenly be destroyed due to the inadvertent or deliberate disclosure of the client's information to unauthorized parties due to a security breach incident (Alagna et al., 2005; Desouza; Salmela, 2008). The exposure of the firm to lawsuits can range in the millions of dollars.

Accordingly, an initial risk assessment should be performed by the law firm's IT Department in order to identify potential threats and vulnerabilities to unauthorized access to PII and confidential data (Ross, 2007; Batista, 2006). An independent third party security firm may also be contracted to perform vulnerability assessments and, thereby, discover the potential risks (Foley, 2008; Heikkila, 2006). If the decision is to hire an IT consulting firm to conduct a security assessment, this typically includes the scheduling of interviews with lead department personnel and/or individual users in all satellite offices as well as the primary location. These interviews provide verification as to whether employees are abiding by the law firm's written security policies and procedures (Humphreys, 2007; ISO/IEC 27002 Joint Technical Committee, 2005). The employees respond to specific questions taken directly from the security policies to assist with ascertaining whether or not these policies are understood and applied correctly (Humphreys) by law firm employees.

Risk assessment results can be categorized by likelihood of occurrence, impact on the firm's tangible and intangible assets, acceptance of risk with remediation, and acceptance

of risk without corrective actions (Humphreys, 2007). Whether the law firm or an independent third party security firm performs the security assessment, the results of this assessment are usually presented to the law firm's managing partners and the IT Department supervisor (Batista, 2006). Managing partners are not typically trained in information security and, therefore, the final risk assessment results must also be presented in a format that is easily understood by the lay-person (Batista; Heikkila, 2006). As noted by Bowen et al. (2006), this report should not consist of accusations about the risks, but rather documentation on actual and projected threats and risks for enabling informed business decisions regarding appropriate corrective controls necessary. The risk assessment should include the review and analysis of compliance with information security policies and procedures by law firm employees.

Participants in the risk assessment process can include those users that remotely access law firm content and information. The various assets of a law firm must be evaluated to determine what the critical assets are and whether or not they are adequately protected (Humphreys, 2007). NIST outlines the various levels of management controls, operational controls, and technical controls that an organization should strive for with its security plan (Bowen et al., 2006). It is important to begin with the mission critical components and develop policies to mitigate any gaps between security risks and corrective actions (Humphreys).

Threat identification includes reviewing the physical or hardware and software components that support access to the law firm's computer systems and network and any vulnerable applications which may perpetuate a security breach incident. Each threat is ranked by the probability of occurrence and whether or not a law firm is willing to accept

the risk, avoid the risk by prohibiting a certain action from being taken, or transfer the risk to an insurance carrier or other third party (Hadfield, 2008; Humphreys, 2007; ISO/IEC 27001 Joint Technical Committee, 2005). Threat probability levels assist with the control analysis, likelihood of occurrences, and impact analysis determination that must be made for each asset (Bowen et al, 2006; Humphreys).

Vulnerability assessments can be conducted with scanning tools that identify the potential risks to the applications, servers, and routers (Batista, 2006; Hadfield, 2008). A penetration test can also assist in identifying how unauthorized users could potentially compromise a law firm's business assets (Bowen et al., 2006). Based on the risks that are identified, the law firm should consider implementing controls to mitigate the threats and vulnerabilities (ISO/IEC 27001 Joint Technical Committee, 2005).

Due care must be exercised when performing vulnerability scans of law firm networks. The potential for exposing a firm's assets during the vulnerability assessment should be determined and guarded against unintended intrusions (Bowen et al., 2006). The tools selected for vulnerability scans may target Microsoft[®] products as well as Cisco[®] and Citrix[®] products that are commonly used in law firm networks (Gibney & Corham, 2008). For example, common vulnerabilities and exposures (CVEs) are found in the Microsoft[®] Internet Information Server (IIS)[®] and Apache[®] Web servers (Whitman & Mattord, 2008). The United States Computer Emergency Response Team (U.S. – CERT) numbers are typically included in vulnerability scan reports. CERT publicly announces vulnerabilities found, as well as the mitigation in the form of patches to remediate these vulnerabilities (Arora, Nandkumar, & Telang, 2006). The published vulnerabilities are assigned numbers for reference purposes. These numbers are divided

into candidate numbers (CAN) and CVE numbers (Carnegie Mellon University, 2008; Pfleeger & Rue, 2008). A CAN is a potential vulnerability, while a CVE is a confirmed vulnerability (Pfleeger & Rue). Thus, the vulnerabilities identified by the vulnerability scan need to be remediated with the appropriate patch to safeguard the law firm network from data leakage and unauthorized access to PII.

Management controls, operational controls, and technical controls safeguard tangible and intangible assets (Bowen et al, 2006). A law firm's reputation and client perceptions are intangible assets (Desouza, 2008). Tangible assets include the law firm's hardware, software, electronic documents, paper documents, and employees (Humphreys, 2007).

Management Controls

Management controls include vulnerability assessments, security policies, and security plans, implemented to manage the security of the law firm's computer systems and network (Bowen et al., 2006). Law firm networks contain financial data, trade secrets, personnel information, client records, including PII and other sensitive data (Comerford, 2006). Protecting this data from disclosure to unauthorized individuals is critical to law firm operations (Ries, 2007). Typically, physical security is the first line of defense that is commonly addressed by law firms (Keller et al., 2005). Critically important is the implementation of security policies and procedures enforced by management to safeguard the integrity of law firm computer information systems (Metzler, 2007). Once a vulnerability assessment is performed and security policies are drafted, a yearly review of the enforcement of security controls is recommended to ensure the adequacy of security controls in mitigating emerging security threats (Humphreys, 2007). Any time a data security breach of a law firm's network has occurred, an assessment should be performed

and the security incident documented and mitigated (Alagna et al., 2005; Humphreys; ISO/IEC 27002 Joint Technical Committee, 2005). According to Humphreys, whenever a new technology is employed by the law firm, an assessment should be conducted to ensure that threats and/or risks associated with the new technology are reduced.

The designation of an individual responsible for security is recommended by ISO/IEC 27002:2005 (ISO/IEC 27002 Joint Technical Committee, 2005). Thus, law firms should consider hiring a Chief Security Officer (CSO) or Information Systems Security Officer (ISSO) to oversee the overall information security of the law firm (Alagna et al., 2005; Bowen et al., 2006). According to Alagna et al., this person should have information security qualifications relative to network access controls, IDSs, as well as information security policies and procedures and be able to communicate IS issues with the lead IT person such as the IT Director or Chief Information Officer (CIO). If a law firm has not developed a security plan or drafted security policies, this may be the first order of business (Keller et al., 2005; Metzler, 2007). A CSO/ISSO oversees the development of security policies and the enforcement of security policies and procedures (Alagna et al.; Bowen et al.; Whitman & Mattord, 2008). At a minimum, one of the current IT Department employees may be designated to assist with vulnerability assessments. Attendance at security training sessions on a regular basis to gain insight on the security risk assessment process and maintain an understanding of the current threats and technical controls available is recommended for the CSO/ISSO (Bowen et al.; ISO/IEC 27001 Joint Technical Committee, 2005; ISO/IEC 27002 Joint Technical Committee; Humphreys, 2007).

Operational Controls

Operational controls include physical security, personnel security, business continuity planning, incident response, hardware and software maintenance, confidential information protection, and security awareness training (ISO/IEC 27002 Joint Technical Committee, 2005) that are implemented by law firm personnel rather than automatically by computer software (Bowen, et al., 2006). The law firm may consider including an audit log requirement in the written security policies with an established protocol for setting up user accounts, including administrative user accounts and passwords (ISO/IEC 27002 Joint Technical Committee; Lin, 2006; Metzler, 2007). Also, written procedures for disabling a user account could be included in the security policies so that a standard process is in place for terminated employee accounts (ISO/IEC 27002 Joint Technical Committee).

With regard to physical security, data centers consisting of network devices and servers should be in a secured area to protect confidential information and PII (ISO/IEC 27002 Joint Technical Committee, 2005; Whitman & Mattord, 2008). For example, highly confidential compact discs (CDs) stored in hallways in plain view pose a threat for theft. Additionally, retired servers must be properly wiped of their contents prior to disposal (FTC Business Alert, 2005; ISO/IEC 27002 Joint Technical Committee). The proper disposal of retired equipment and the locking of server rooms, as well as the safe storage of CDs should be included in the security policies to provide appropriate procedures for protecting law firm PII and confidential information (ISO/IEC 27002 Joint Technical Committee).

Enforcing an encryption policy to ensure the encryption of data at rest and on laptops, as well as USB devices (Radcliff, 2008; Myler & Broadbent, 2006) is another operational control for law firms. Access to confidential information residing on the law firm network and removable media devices can be mitigated by installing encryption software on hard drives as well as USB devices (Radcliff; Heikkila, 2007). The benefit of encrypting PII and sensitive data is that the state security breach notification laws, with the exception of Wyoming, specifically exempt notices to clients if the compromised PII is encrypted and the encryption key is not attached (Greenberg, 2008).

In the absence of training or educational sessions regarding security issues, law firm employees may lack procedures or policies covering the basic functions, such as changing the default passwords issued to each user (Gupta & Hammond, 2005). This absence results in a large numbers of users who never change default passwords (Gupta & Hammond; Metzler, 2007). One corrective action could be implementing the requirement that the login password be changed upon the first login session (ISO/IEC 27002 Joint Technical Committee, 2005). The operational control of changing passwords has met with some resistance (Keller et al., 2005) from law firm users (M. Thorogood, personal communication, December 18, 2008). However, law firm IT departments must develop, implement, and enforce password policies that will assist with mitigating this risk (ISO/IEC 27002 Joint Technical Committee; Whitman & Mattord, 2008).

Further consideration as to the number of times a password must be changed should coincide with the sensitivity of the data being protected and the feasibility of users changing, as well as protecting, their passwords (ISO/IEC 27002 Joint Technical Committee, 2005; Whitman & Mattord, 2008). From time to time, a law firm may

employ many contract attorneys to work on litigation support databases (Gorga & Halberstam, 2007) who have access to sensitive data. In these types of situations it is important that the passwords change more often. It is difficult for people to remember their passwords due to the number of passwords required on various Websites (Richardson, 2006), as well as at the law firm. According to Harrison (2006) a 2006 Sophos survey found that “41 percent of the respondents said they always use the same password, 45 percent said they have a few different passwords, and 14 percent said they never use the same password on multiple Web sites” (p. 5). Strong passwords require a combination of lower case letters, upper case letters, as well as a mix of numbers and/or other characters found on a keyboard (Basta & Halton, 2008; Harrison; Keller et al., 2005; Richardson). Training on how to choose and maintain a strong password is advisable for all law firm employees and mandatory particularly for all temporary contract attorneys (Gorga & Halberstam; Heikkila, 2006), especially those with access to PII and sensitive data.

Technical Controls

Technical controls are those security controls, such as access controls, audit logs, and user authentication that assist with the detection of security violations by automated software programs (Bowen et al., 2006; ISO/IEC 27002 Joint Technical Committee, 2005). Technical controls, such as anti-virus software, IDSs, and data leakage content filtering, assist with enforcement of law firm security policies (Whitman & Mattford, 2008).

Audit logs are incorporated within software packages and merely need to be enabled in order to log the events that have occurred within a computer program (ISO/IEC 27002

Joint Technical Committee, 2005; Kent & Souppaya, 2006). For example, data leakage software can identify whether SSNs or credit card numbers are being sent within the contents of an unencrypted e-mail message (Hook, 2009). This data leakage software will prohibit and/or stop the e-mail from being successfully sent out. It will also send an automated e-mail to the sender stating that the inclusion of SSNs, credit card numbers or other PII is a violation of law firm policies as well as certain laws (Hook). Event logs are reviewed to determine if a security breach has occurred and to assist with the investigation of an incident (Kent & Souppaya). Additionally, audit logs may act as a preventative tool if law firm employees are aware that their actions are being logged.

Summary of What is Known and Unknown about the Topic

Security policies allegedly help with preventing security breach incidents (Baker & Wallace, 2007; Da Veiga & Eloff, 2007; Doherty & Fulford, 2005; Hong et al., 2006; Keller et al., 2005; Metzler, 2007; Myler & Broadbent, 2006; Verdon, 2006). Doherty and Fulford found no statistical relationship between security policies and security breach incidents. However, they did not examine whether or not the security policies were initiated by the security breach or were already in place when the security breach incident occurred.

Wiant (2005) investigated the existence of information security policies in hospitals and their value in prompting hospital employees to report security incidents. This survey had a 5.6% completed response rate to their mail surveys. Wiant found that those hospitals with information security policies did not have fewer incidents or less serious incidents of computer abuse than those hospitals that had no information security policies at all. Wiant suggests that the legal industry is behind in security initiatives and

recommends further research with regard to the effectiveness of information security policies in abating security incidents.

Regulatory compliance requires sensitive data be adequately safeguarded from inadvertent disclosure and supports the availability of audit trails to monitor who has access to data (Bowen et al., 2006; Greene, 2006). Laws requiring administrative, physical, and technical safeguards for compliance include 45 state security breach notification laws as of October 2009 requiring notification of unauthorized access to computerized PII (Greenberg, 2009). These security breach notification laws are similar to SB 1386 (2002), GLBA (1999), HIPAA (CMS, 2003), and SOX (2002). Law firms have clients who must comply with these regulations. When protected data are transferred to the law firm by the client, the law firm must also comply with the regulations and provide adequate safeguards (Comerford, 2006). Law firms must abide by applicable state security breach notification laws with regard to their employee records in the event employees' SSNs, bank accounts, or other financial information is breached (Johnson, 2008; Kugele & Placer, 2007; Schwartz & Janger, 2007).

The Contribution This Study Will Make to the Field

There is little empirical research on information security policies and their effect on computer security breach incidents (Doherty & Fulford, 2005; Hagen et al., 2008; Hong et al., 2006; Kemp, M., 2005; Romanosky et al., 2008; Thomson, K-L & von Solms, R., 2006; Wiant, 2005). The contribution of this dissertation investigation is the furtherance of the research of Doherty and Fulford, as well as Wiant with a different population and discovery of whether information security policies created proactively aided in preventing security breach incidents.

Surveys of different populations have produced varied results concerning security (Pfleeger & Rue, 2008). Hong et al. (2006) determined in a study of companies in Taiwan that “Organizational type will have an impact on the time of building an ISP [information security policy]” (p. 111) and “The larger size of MIS department of an organization, the earlier will this organization build an ISP” (p. 11). According to Siponen and Oinas-Kukkonen (2007), research has historically concentrated on the technological perspective; and additional research is needed with regard to practical observations of security management. In a study of companies in Norway, Hagen et al. (2008) determined security measures are interdependent. According to Albrechtsen et al., the implementation and effectiveness of security measures result in an inverse relationship and “This inverse relationship is interpreted as a metaphorical staircase of four steps: security policy; procedures and control; tools and methods; and awareness creation” (p. 393). The author’s findings regarding the effectiveness of information security policies in reducing the number of computer security breach incidents will contribute to the body of knowledge and provide data concerning the perception of law firms, an under represented population, in the information assurance field.

The author also added to the body of knowledge with regard to security breach notification laws. Although information assurance is evolving with regard to computer security breach incidences (Pfleeger & Rue, 2008; Romanosky et al., 2008; Wiant, 2005), this research is valuable because it provides insight concerning the effect that information security policies have on computer security breaches in law firms. The proliferation of security breach incidents has substantially and rapidly risen over the past five years (ITRC, 2009; Open Security Foundation, 2008; Romanosky et al.). In the U.S.,

individual State data breach notification laws protect the PII of individuals and subsequently require notification to state residents of possible compromises that may lead to identity theft. Unlike other data privacy laws that are industry-specific, such as GLBA (for financial services) or HIPAA (for healthcare), these individual state laws are applicable to any industry, including the legal industry. The one significant finding of this dissertation investigation in regard to the state security breach notification laws is that law firms demonstrated a need to become more immersed in security breach notification law requirements with regard to the requirement that notification of a security breach of computerized data is based on where the resident resides rather than where the data reside (Romanosky et al.) in order to respond appropriately to any unauthorized access to client data or employee PII. The results also demonstrated a significant difference between the small and medium, small and large, small and very large law firms with regard to who encrypts e-mail messages with the small law firms reporting less usage of encryption of e-mail messages and hard drive data. While this is not a surprising finding given the financial constraints of small law firms, it does provide insight for legislators to apply when they consider passing laws mandating that all PII data inserted into e-mail messages or stored on hard drives be encrypted (Worthen, 2008).

In this dissertation investigation, the author contributed to the body of knowledge with regard to an affirmation of literature regarding self-efficacy (LaRose et al., 2008). This dissertation confirmed that users are unmotivated to download security software while in the middle of a project or they feel incapable of making an appropriate decision with regard to whether or not they should install security software (West, 2008).

Chapter 3

Methodology

Research Methods Employed

This dissertation investigation utilized a Web-based survey to document and analyze the responses of law firm IT personnel with regard to their perceptions of how information security policies affect computer security breach incidents. The author investigated the exploratory analysis study of Doherty and Fulford (2005), who surveyed IT directors from large U.K.-based organizations (employing more than 250 people) regarding the role of information security policies in relation to the number and severity of security breaches. The author incorporated the Doherty and Fulford original survey instrument and compared those results to the data collected in this research. The relationship between information security policies and information security breach incidents was also examined. Validated questions from the Doherty and Fulford survey were adapted into this dissertation study. Survey questions regarding security threats, security policies, and successful implementation of information security policies were adopted from the original survey instrument received from Doherty and Fulford. Additional questions posited by the author included self-efficacy issues, applicable privacy laws, management approval and communication of security policies, and utilization of risk assessments and other security measures in law firms (Post & Kagan, 2007; Myler & Broadbent, 2006; Verdon, 2006). Furthermore, the author investigated

the role of IT security assessments utilized by law firms in assuring that their networks are protected from possible information security breaches.

Specific Procedures Employed

Online Survey Development and Distribution

The author developed and distributed a Web-based survey by utilizing Zoomerang (www.zoomerang.com), a Web survey tool. Global law firm IT members of ILTA were surveyed. Data were collected from the Web-based questionnaire with multi-choice questions, demographic questions, and Likert-scale questions. As required whenever using human subjects, the author completed the institutional review board (IRB) process (Patton, 2002) with the Nova Southeastern University (NSU) IRB. The author's survey received initial NSU IRB approval on April 15, 2008 and on January 7, 2009 an Amendment of IRB Approved Studies (NSU IRB Protocol, 2008) was approved (see Appendix C).

The author developed a set of questions based on current information security policies and security breach notification laws (Gibney & Corham, 2008; Greenberg, 2009; Myler & Broadbent, 2006; Post & Kagan, 2007; Verdon, 2006; Wiant, 2005). The original questions from the Doherty and Fulford's (2005) study were validated in a pre-test and a post-test conducted by Doherty and Fulford. This set of questions was included in the author's Web-based survey on Zoomerang. Five-point Likert-scale questions for the questionnaire contained five responses including a neutral response available in-between the *strongly agree* on one end and *strongly disagree* on the other end (Sekaran, 2003).

The variables in this dissertation investigation were information security policies, information security breach incidents, updating information security policies, revising

information security policies, adoption of best practices, self-efficacy, security measures, and law firm size. According to Creswell (2009), relating the variables to research questions and specifically to survey instrument items aids the author in expressing how the research question answers were calculated. This investigation's variables, research questions, including the corresponding survey questions, are outlined in Table 3.

Table 3. Variables, Research Questions, and Items on Author's Survey

Variable Name	Research Question	Item on Survey
Information Security Policies and Security Breach Incidents	1. Do law firms that have written information security policies have fewer security breach incidents in terms of frequency and severity than those that do not have information security policies (Doherty & Fulford, 2005, p. 25)?	See Questions 3, 11, 12
Information Security Policies and Security Breach Incidents	2. Are law firms that have had information security policies in place for numerous years likely to have fewer computer security breach incidents in terms of both frequency and severity than those that do not have information security policies in place (Doherty & Fulford, 2005, p. 25)?	See Questions 3, 11, 12, 16
Updated Information Security Policies and Security Breach Incidents	3. Do law firms that have updated their information security policies on a regular basis have fewer security breach incidents in terms of frequency and severity than those that have not updated their information security policies (Doherty & Fulford, 2005, p. 26)?	See Questions 3, 11, 12, 17
Information Security Policies and Security Breach Incidents	4. Are law firms that have an information security policy with a broad scope likely to have fewer security breaches in terms of both frequency and severity than those organizations that do not (Doherty & Fulford, 2005, p. 26)?	See Questions 3, 11, 12, 21, 22
Adoption of Best Practices and Security Breach Incidents	5. Are law firms that have adopted a wide variety of best practices likely to have fewer security breaches in terms of both frequency and severity than those organizations that have not (Doherty & Fulford, 2005, p. 26)?	See Questions 3, 11, 12, 21, 22, 23, 24, 25, 26, 27
Self-efficacy	6. When under a time deadline to finish an assignment, are law firm employees more likely to by-pass security measures in order to complete the task (Post & Kagan, 2007)?	See Questions 3, 28

Variable Name	Research Question	Item on Survey
Information Security Policies and Security Breach Incidents	7. Are law firm security policies created in response to an information security breach incident (Doherty & Fulford, 2005; Wiant, 2005)?	See Questions 3, 13, 14, 15, 29
Security Measures and Information Security Policies	8. Are risk assessments, network vulnerability scans, and/or penetration tests a part of law firms' validation of the intended security policies (Myler & Broadbent, 2006; Verdon, 2006)?	See Questions 3, 18, 19, 20, 30
Information Security Policies and Law Firm Size	9. Do larger law firms (more than 251 users) and smaller law firms (less than 250 users) differ in whether they have written information security policies (Gibney & Corham, 2008)?	See Questions 3, 14
Information Security Policies, Security Breach Incidents, and Law Firm Size	10. Do smaller law firms (less than 250 employees) and larger law firms (more than 251 users) differ in whether written information security policies were due to information security breach incidents (Gibney & Corham, 2008)?	See Questions 3, 14, 15

The remaining questions posed in the author's online survey included demographic questions as to size of the IT department, location(s) of the firm offices, functions of law firm technology related departments, designation of security responsibility, education, gender, age, job level, length of experience, position at the law firm, and privacy and/or security law compliance requirements.

The author's online survey was distributed through an e-mail message from the ILTA's Executive Director, Randi Mayes, to its members via its membership database of law firm technology professionals that included a link to the author's Zoomerang survey. By having the cooperation of ILTA (see Appendix D), the survey was more credible and well received by its members (Baker & Wallace, 2007), instead of coming directly from a lesser known sender. In an effort to encourage responses, Ms Mayes provided a link to the ILTA Website where a PDF of the survey questions was available for ILTA members to preview prior to participating in this dissertation study. As of April 2009, 1,123 law

firms globally held ILTA memberships. The author utilized Zoomerang.com to host this survey since ILTA members are familiar with completing the annual ILTA technology surveys using the Zoomerang interface. The questionnaire was formatted in hypertext markup language (HTML) and uploaded to the Zoomerang.com Website. The 35 question survey distributed to ILTA members is attached as Appendix E.

According to Roster et al. (2007), online surveys are more cost efficient and provide more design features than paper surveys. Evans and Mathur (2005) and Punter, Ciolkowski, Freimut, and John (2003) point out the advantage of the simplicity with which the respondents are able to complete the online survey as well as how quickly the researcher can analyze the results since they are already in an electronic format. With the results already provided in electronic format, the reliability of the data collected from the online survey is improved since the results are not hand coded (Punter et al.). The simplification of responding to the author's Zoomerang.com link provided by ILTA, where the respondents merely click on their answers, improves the response rate as compared to mailed paper surveys (Punter et al.). Evans and Mathur further found that online surveys are more convenient than mail surveys or interviews because they can be completed at the respondent's leisure and thus are more likely to be completed.

Sampling and Participants

The population for this online survey consisted of law firm IT personnel and others familiar with legal technology in law firms. Fulford and Doherty (2003) found that surveys targeting IT personnel "yield a more realistic assessment of the information security situations in an organization" (p. 107). In this online survey, the author

continued to use firm size defined in ILTA's 2008 Technology Survey (Gibney & Corham, 2008, p.3.) as:

Firm size	Number of users
Small	<151
Medium	151-250
Large	251-500
Very Large	>500

Participants were provided a letter describing the research and an Informed Consent Form as the first page of the survey. Subjects were recruited from the global ILTA membership. By including law firms outside of the U.S., the author was provided an opportunity to gather and analyze data on an international level. Attorneys, paralegals, and law firm IT staff who consented to participate in the dissertation investigation constituted the research subjects. Thus, a site selection purposeful sampling was utilized by targeting ILTA legal technology members who were knowledgeable and skilled in using their law firm's IT (Sekaran, 2003).

ILTA agreed to assist with ensuring that only one e-mail invitation to take this questionnaire was sent to each law firm, despite multiple offices across the globe (see Appendix D). The information obtained in this dissertation investigation was treated as strictly confidential unless disclosure is required by law. The participant's name was not linked to his/her responses and was not used in the reporting of information in publications or conference presentations. The names of subjects or e-mail addresses of the respondents were not known to the researcher since ILTA sent out the invitation. However, there was an opportunity for the respondents on the questionnaire to provide the author with their e-mail addresses for possible follow-up questions. Nevertheless, their names and any other identifying information provided were not used in the reporting

of information in this dissertation, in any publications, or conference presentations. Only cumulative results were analyzed and placed into this dissertation.

Participation in this dissertation investigation by members of this legal technology group was on a random, volunteer basis, inasmuch as not every member who received the e-mailed link to the questionnaire completed it (Patton, 2002). The author offered a copy of the results to participants as an enticement to participate (Baker & Wallace, 2007).

Data Collection

Online survey questions elicited responses to direct questions concerning whether or not information security policies developed for law firm personnel affect security breach incidents. Questions dealing with how security is handled, what security measures are in place, types of security breaches the law firm has encountered, and security policies utilization in law firms were posed to all participants.

Survey results were placed in the Zoomerang database on www.zoomerang.com, and were only available online to the author via an ID and a password. The raw data results were then exported from the Zoomerang database into a Microsoft® Excel® spreadsheet. Confidentiality was maintained by the anonymity of the results provided on this Zoomerang account and no identifying information of the respondents was transferred to NSU.

Data Analysis

The survey results were tabulated using Statistical Package for the Social Sciences (SPSS™)12.0 for the advanced statistics, as well as SPSS™ PASW® Statistics 17.0 for Microsoft® Windows®, and Microsoft® Excel® 2007 software's statistical functions to create tables representing the respondents' responses. An interpretation of these results in

the form of a narrative addresses responses to the research questions and include tables (Creswell, 2009) created using both SPSS™ and the statistical functions of Microsoft® Excel® 2007. Data analyses are provided in a narrative form that included an interpretation of the findings (Creswell).

Assistance with the analysis of the advanced statistics of this study's results was provided by Dr. Phyllis Curtiss, Director of the Grand Valley State University (GVSU) Statistical Consulting Center (SCC). Dr. Curtiss had access to the raw data Microsoft® Excel® spreadsheet containing the individualized responses of the respondents, which was loaded onto a GVSU secure server that requires userid and password to access the data. This spreadsheet was utilized to calculate the advanced statistics and was safeguarded by limiting access to the file at the SCC to only Dr. Curtiss and those students generating the statistics under the direction of Dr. Curtiss. Upon completion of the advanced statistical calculations, this file was securely deleted from the GVSU SCC computers and network.

The Role of the Researcher

According to Creswell (2009), the background of the researcher in qualitative studies should be included in the study to provide an understanding of how past experiences may influence the interpretation of the dissertation investigation. The author has firsthand knowledge of the evolution from paper documents exchanged during litigation to the current trend of electronic document production with 18 years of experience as a paralegal in two law firms in Michigan. Most recently achieving her Certified Information Security Manager (CISM), Certified Information Privacy Professional (CIPP) certification, as well as experience as a law firm Information Technology (IT)

Project Manager, and Information Security Consultant, the author has been exposed to the numerous information security policies, security breach incidents, data privacy laws, and security breach notification laws. The issue of security and confidentiality of sensitive client information and PII is of primary concern to a law firm.

Reliability and Validity

According to Sinkovics, Penz, and Ghauri (2008), reliability is more objective than subjective in qualitative research. Sinkovics et al. suggest building on a previous study as a way to remove method bias. The author furthered the study of Doherty and Fulford (2005) in an attempt to remove this validity issue. According to Creswell (2009), member checking of themes discovered from the investigation should be presented to someone involved with the group taking the survey. To further enhance the validity of the Web-based survey, the author used member checking with the 2007-2009 ILTA President and Sidley Austin LLP's Enterprise End User Services Director, Joy Heath Rush, to ensure the accuracy of the findings (Creswell). Additionally, through peer debriefing and peer review, the author ensured the validity of the findings of the study with Meg Hackett, J.D., a lawyer in a law firm who did not participate in the online survey (Creswell). By surveying a diverse population of IT law firm personnel across the U.S. the author further ensured the corroboration of the Web-based study (Creswell & Clark, 2007; Patton, 2002).

Importantly by incorporating the Doherty and Fulford's (2005) original survey instrument into this dissertation investigation, the author also validated the findings obtained by Doherty and Fulford within the legal sector (Patton) and also demonstrated the reliability of this earlier survey (Creswell, 2009). Doherty and Fulford validated their

survey instrument through two pre-tests and a pilot study exercise distributed to experienced IS researchers and senior IT professionals with IS duties. A panel of subject matter experts provided input as to the validity and reliability of the author's survey questions as well. The subject matter expert panel included:

1. Anne K. Abatte – Ph.D., Executive Director Greater Cincinnati Library Consortium, Cincinnati, Ohio
2. Ruth S. Stevens, M.L.S, J.D., Associate Professor, Grand Valley State University, Grand Rapids, Michigan
3. Mark Thorogood, M.S. – Manager, Application Services at McDermott Will & Emery LLP, Chicago, Illinois

The subject matter experts' comments (see Table 4) formed the foundation for the revision of the original survey. The author's survey (see Appendix E) primarily incorporated the questions from the original survey instrument (see Appendix F) developed by Doherty and Fulford's (2005) to support their empirical study regarding security breaches and security policies. Appendix G shows the redline revisions made to the Doherty and Fulford original survey instrument. These changes enabled the author to customize the original survey to match the research questions for this dissertation research.

Table 4. Feedback from the Subject Matter Experts That Served as Panel Members

<i>Question</i>	<i>Comment</i>	<i>Resolution</i>
1 How many lawyers are employed by your law firm?	"Small" should be smaller--you may insult someone with numbers that large. Why are these law firm size numbers significant? Why have break between 150 and 151 vs. 100 and 101, etc. Are these categories used by another survey or group?	ILTA audience uses these terms on a regular basis. No action taken. The target audience is familiar with these law firm sizes since ILTA uses these sizes on all of their surveys.

<i>Question</i>	<i>Comment</i>	<i>Resolution</i>
	The term “employed” in the question may be confusing. By definition, partners are not employed, they are self-employed. In a typical law firm, only counsels, non-attorney professionals, and associates are employees of the firm. Partners are business owners, not employees.	Revised the question to: “Please indicate the size of your law firm.”
	Wouldn’t the size of the IT department be important as well?	Yes, added this question.
	Change the sentence “How many lawyers are employed by your law firm?” to “Indicate the size of your law firm?”	Revised the question to: “Please indicate the size of your law firm.”
	Inside the table, change “Number of Users” to either “Number of End-users” or “Number of Lawyers.” Note that the term “attorneys” should not be used because it means different things depending upon the nationality of the reader. For example, there are attorneys, barristers, and solicitors in the United Kingdom. Additionally, the term “employed” should not be used because technically partners are business owners, not employees. Lastly, the term used in the table should agree with the term used in the question. The terms presently do not agree.	ILTA’s Executive Director indicated via e-mail that she believes number of users is a more accurate depiction of firm size. Revised attorneys to law firm employees/lawyers or other members of the firm throughout the survey.
	Is the size breakdown consistent with other surveys?	The target audience is familiar with these law firm sizes since ILTA uses these sizes on all of their surveys.

<i>Question</i>	<i>Comment</i>	<i>Resolution</i>
2 Which of the following most accurately describes the location(s) of your firm's offices?	Why do you switch from "global" to "international" in the responses? This could be confusing.	Changed all responses to "international."
	Does this mean an office outside of the U.S.? Global typically means comprehensive. The terms global and international may be confusing. The term "global" appears to mean non-U.S. office; however, the term could also mean servicing clients from multiple nations, which is sometimes done, especially when dealing with intellectual property matters before the Europe court.	Changed all responses to "international."
	The question seems to be tapping two dimensions (i.e., office count and office locations). The question could be severed into two questions, thereby making it clearer.	Revised question to: Please indicate the size of your law firm information technology department. Added a new Question 3: Which of the following most accurately describes the location(s) of your firm's offices?
Added a new Question 3: Which of the following most accurately describes the location(s) of your firm's offices?		
4 Which of the following best describes your law firm?	None.	
5 Which of the following technology-related department(s) does your law firm have?	Get rid of "but" in the last choice- -Seems confusing, and perhaps says that a different name is wrong.	Revised question to list functions rather than department titles.

<i>Question</i>	<i>Comment</i>	<i>Resolution</i>	
	I am concerned about the wording of this question. Should this be a list of functions, not department titles? I see a situation in which departments at two different firms have the same titles, but they do different things.		
	What is the difference between information technology and information systems? Moreover, many firms call their IT department Information Services. This raises the concern of synonyms and the need to clarify terms and concepts that are potentially ambiguous.	Changed “information systems” to “information services.”	
	What about a large office that does not have departments?	Changed to a list of functions.	
	The list of departments appears to contain synonyms, which may cause confusion.	Revised.	
	Are you only interested in services that relate to information security? If so, you should state that. If you want all services, you might get a lot of responses in your "Other" category, like training, hardware installation, upgrade, etc.	Added information security to question: “Which of the following information security functions does your law firm technology-related department(s) provide?”	
6	Does your law firm have a designated person or a group of people who handle security issues?	Are you only interested if they have one person? What if they had two people or a whole department? How should they answer the question?	Changed to have two “yes” answers – one for a single person and the other for a group.
7	If yes, what is their title?	None.	

<i>Question</i>	<i>Comment</i>	<i>Resolution</i>
8 Which of the following privacy and/or security laws is your law firm required to comply with?	I think there should be a "Don't Know" option next to each option. They might know about one law they have to comply with but not about another.	Added a "Do not know" selection.
9 Please record in the table below the approximate number of IT security breaches that your law firm has experienced in the past two years.	None – this question is from Doherty and Fulford's original UK study on Info. Security Policies survey instrument.	
10 Please indicate the severity of the worst breach of each type that your law firm has experienced in the past two years, using the scale provided.	None – this question is from Doherty and Fulford's original UK study on Info. Security Policies survey instrument.	
11 Please indicate your level of agreement with the following statements.	None – this question is from Doherty and Fulford's original UK study on Info. Security Policies survey instrument.	
12 Does your law firm have written information technology (IT) security policies?	None – this question is from Doherty and Fulford's original UK study on Info. Security Policies survey instrument.	
13 Were your law firm written IT security policies and procedures created due to a security incident/breach?	None.	
14 How long has your law firm been actively using a documented IT security policy?	None – this question is from Doherty and Fulford's original UK study on Info. Security Policies survey instrument	

<i>Question</i>	<i>Comment</i>	<i>Resolution</i>
15 Approximately how often is the IT security policy updated?	None – this question is from Doherty and Fulford’s original UK study on Info. Security Policies survey instrument.	
16 Does your law firm audit and enforce the documented IT security policy?	None.	
17 Approximately how often is the IT security policy audited by an independent third party?	I don't like the sequencing of the responses. They should be in order of frequency from least to highest. Every two years should be before less than every two years. I also don't like your intervals. I think there are gaps and combining "more" and "less" could create confusion. How about specific ranges. Every two years or more. Between one year and 2 years, etc. Whatever you want to know.	Revised the sequencing of frequency from least to highest.
18 How is the IT security policy disseminated to law firm employees/attorneys?	None – this question is from Doherty and Fulford’s original UK study on Info. Security Policies survey instrument.	Revised “organization employees” to law firm employees/lawyers or other members of the firm.
19 Using the table below, please indicate the security issues covered in your IT security policy and/or through separate procedures or standards. If you do not explicitly cover an issue through your policy or a separate stand-alone standard, please leave blank.	None – this question is from Doherty and Fulford’s original UK study on Info. Security Policies survey instrument.	

<i>Question</i>	<i>Comment</i>	<i>Resolution</i>
20 How important do you believe the following factors to be for the successful implementation of IT security in your law firm on a scale of 1-5 with 1 being the least important and 5 being most important?	None – this question is from Doherty and Fulford’s original UK study on Info. Security Policies survey instrument.	Revised “organization” to law firm.
21 How successful do you believe your law firm has been in adopting each of these factors on a scale of 1-5 with 1 being the least important and 5 being most important?	None – this question is from Doherty and Fulford’s original UK study on Info. Security Policies survey instrument.	Revised “organization” to law firm.
22 Are IT security policy documents approved by management, published and communicated to all law firm employees and relevant third party service providers? Added a new Question 22: Are IT security policy documents approved by management?	I think this combines too many things in one question. How separating it into three questions 1 approved 2 published 3 communicated	Split old question 22 into three questions as recommended.
23 Added a new Question 23: Are IT security policy documents published?		Split old question 22 into three questions as recommended.

<i>Question</i>	<i>Comment</i>	<i>Resolution</i>
24 Added a new Question 24: Are approved IT security policy documents communicated to all law firm employees and relevant third party service providers?		Split old question 22 into three questions as recommended
25 Are law firm computers shut down for inactivity after a defined period?	None.	
26 When under a time deadline to finish an assignment, how likely would it be to:	In this question you don't say who you are referring to. Is the person supposed to answer based on what they would do or what they think other people in their firm would do?	Changed to add to: how likely would it be "for people in your law firm."
27 Please indicate your level of agreement with the following statements: . . .	Are you asking about both policies and procedures? Is the question whether or not firms need written policies or whether they need procedures to protect information security or both? Could you just leave out the word "procedures"?	Deleted procedures.
28 During the past 12 months, how often did your law firm . . . ?	I would highlight "past 12 months" to make it easier to see. Do you need a "don't know" option? Should this question include instructions such as select the answer that best applies because the potential responses are not collectively exhaustive?	Highlighted on Word document and on Zoomerang. Added a "Do not know" column. Revised to, "During the past 12 months, how often did your law firm? Select the answer that best applies".

<i>Question</i>	<i>Comment</i>	<i>Resolution</i>
	“A Few Times a Month” – Should this be “more than once per month”?	Revised to “more than once per month”.
29		
Which of the following statements is true for your law firm?	I would switch the order on your last two choices. This leads to sort of a natural progression.	Switched order of last two choices.
Section 4 header Demographic Questions These last few questions are to help me get to know you, the respondent better. Like all of the questions in this questionnaire, your answers were held in strict confidence. No answers were paired with an individual and only a cumulative set of results were presented in the dissertation.get to know you, the respondent, better. . . Are these required or optional? Do you want to state that they are optional? I might be put off by this type of question, but I understand why you are trying to get this information.	Added comma after “respondent”. Added: All of these responses are optional.
30		
What is the highest level of education you have completed?	"Highest level" could be difficult for someone. What if they have a bachelors and a JD? Does "highest level" assume that they also have a master degree? Are these categories (Ph.D.) necessary, particularly the A.B.D. category?	Added: “Prefer not to answer” to level of education. Removed A.B.D.
31		
Please state your gender.	None.	
32		
Please state your age.	None.	
33		
Which title best describes your job level?	Can you add "Law Firm Administrator" or even CEO as one of the options?	Yes, added “Law Firm Administrator” and “Chief Executive Officer”.

<i>Question</i>	<i>Comment</i>	<i>Resolution</i>
<p>34</p> <p>Would you be willing to be contacted to answer follow-up questions via an e-mail message linking you to a second follow-up Zoomerang survey, if necessary?</p> <p>* Please note that your e-mail address will only be used to send you the link to the additional survey. Any and all additional information obtained would be held in strict confidence and your name would not be used in the reporting of information.</p>	<p>None.</p>	
<p>Final Paragraph</p> <p>Thank you for participating in this study! Is there anything additional that you would like to share with the researcher? Please provide your comments in the space provided.</p>	<p>When I started looking at the survey, one of my first thoughts (as a potential respondent) was whether my responses would be confidential. I think there should be a reminder at the beginning of the survey (not just the cover letter) that responses are confidential and will not be linked to any particular firm or person. If I were in law firm IT, I would be very hesitant to share details about my firm's security procedures that could be leaked to others.</p>	<p>Added confidentiality clause to first question and end of survey.</p>

Threats to Internal Validity

The primary internal validity threat to this dissertation investigation was maturation. Sekaran (2003) defines maturation as the tainting of the survey results due to an uncontrollable variable such as the passage of time. Since technology is evolving at a

rapid pace, the threat of maturation effects through the passage of time as the dissertation investigation continues (Sekaran) coupled with technology changes is also a concern. The survey questions were posed to a panel of subject matter experts in an attempt to control this threat. The length the survey was open to the respondents was also limited to three weeks in an effort to combat maturation effects.

Threat to External Validity

A threat to external validity for this dissertation investigation was selection threats of having more than one person from the same law firm complete the questionnaire. In an attempt to control this threat, ILTA agreed to send the link to this Web-based study to only one e-mail address per law firm (see Appendix D). Additionally, an external validity threat that could not be controlled by the author was whether or not the person who received the link to the questionnaire was the actual person who completed the questionnaire.

Formats for Presenting Results

The data collections were represented in graphical format and tables. SPSS™ 12.0 was utilized for the advanced statistics, as well as SPSS™ PASW® Statistics 17.0 for Microsoft® Windows® and the statistical functions of Microsoft® Excel® 2007 to analyze and calculate the results of the questionnaires. The survey results were provided to the researcher from the Zoomerang software in a format that was easily converted into SPSS™ and Microsoft® Excel® 2007 for analysis and computation of results using the various statistical features of these software programs.

Resource Requirements

Randi Mayes, the ILTA Executive Director, assisted with the distribution of the surveys to the ILTA members by distributing an e-mail invitation with the link to the author's Zoomerang Website (see Appendix D). Reminder e-mails to complete the study were sent by Ms. Mayes. Zoomerang sent the online results only to the author. Access to the data collected on Zoomerang was password protected and limited to the author.

Dr. Phyllis Curtiss, Director of the GVSU SCC and those students generating the advanced statistics under her direction had access to the raw data Microsoft® Excel® spreadsheet containing the individualized responses of the respondents. This raw data spreadsheet was provided by the author and loaded onto a GVSU secure server that requires userid and password to access the data. This spreadsheet was utilized to calculate the advanced statistics using SPSS™ 12.0. Participants were not identified in any of the results. Additionally, SPSS™ PASW® Statistics 17.0 for Microsoft® Windows® and Microsoft® Excel® 2007 were used to analyze and calculate the results of the questionnaires.

Internet access to the Zoomerang Website account to set up the survey and review the results of the survey as well as e-mail to send out the Zoomerang link to Randi Mayes were necessary resources. The NSU electronic library (e-library), the Internet, and articles in professional journals and magazines supported the author's research in this topic area.

Summary

In this chapter the author delineated the specific procedures employed for conducting the survey and analyzing the survey findings. The author described the methodology

utilized for this investigation. The approach consisted of the development and distribution of a Web-based survey that was based on the Doherty and Fulford (2005) survey and included additional new questions posited by the author. The use of Zoomerang as the online survey tool and the agreement with ILTA to send out e-mail invitations to their members was also described.

Furthermore in this chapter, the author discussed the data analysis conducted with regard to the results received from the Zoomerang survey. The composition of the target population and sampling for this study was described. The reliability and validity of the research was reviewed, including the feedback received from the subject matter experts that served as panel members with regard to customizing the Doherty and Fulford (2005) questions for this dissertation investigation. Resource requirements and IRB approval processes were also examined.

Chapter 4

Results

Introduction

This chapter reviews the findings of this dissertation investigation which was designed using the original survey instrument from the Doherty and Fulford (2005) study along with some additional questions posited by the author. The survey was converted to an online survey, hosted on Zoomerang. The analysis of these responses includes an analysis of their relationship to the Doherty and Fulford responses.

On March 12, 2009, ILTA Executive Director, Randi Mayes, sent out an invitation to 1,123 ILTA members to partake in the author's Web-based study by providing the ILTA members with an introduction to the author and a link to the Zoomerang online survey. Ms. Mayes included a link to the ILTA Website where a copy of the survey could be previewed prior to taking the survey. Ms. Mayes also sent out notices on March 20, 2009 and April 1, 2009 reminding all 1,123 ILTA members to complete the author's survey on Zoomerang. This survey was open for three weeks. Those who completed the survey and agreed to respond to additional follow-up questions were sent an additional Zoomerang link to these questions on April 2, 2009. Follow-up questions were open for two weeks. Overall, data were collected over a five week timeframe ending April 15, 2009.

A total of 111 ILTA members initiated responding to the online Zoomerang survey. Of these, there were 19 people who completed only a portion of the survey. These incomplete responses were not included in the response rate or percentage calculation for valid responses (Sekaran, 2003). There were 92 *completed* responses to the survey received, of which four *completed* the survey by declining to participate after reading the informed consent resulting in 88 valid responses. The response rate for the survey was 8.19% (92 *completed* responses) with 7.83% (88) of the respondents providing valid responses.

It is interesting to note that the Doherty and Fulford study response rate was 7.7%. Wiant's (2005) investigation had a 5.6% completed response rate to mail surveys regarding the existence of information security policies in hospitals and their value in prompting hospital employees to report security incidents. The Computer Security Institute (CSI) response rate for their 13th year of its CSI Computer Crime and Security Survey (2008) was 10%. Similar to the Doherty and Fulford study, as well as the Wiant studies, when CSI first deployed their survey in 1996, their response rate also was low at 8.6% (Power, 2002).

The author supplemented the dissertation investigation with follow-up questions sent to 45 of the respondents that had provided e-mail addresses for this purpose. The author asked the open ended question: "Why do you think so few people respond to questionnaires dealing with security?" A number of the respondents stated that it was due to fear of disclosing vulnerabilities, exposure, or liability concerns. The table below created from data received from follow-up questions shows the actual responses:

Table 5. Open Ended Follow-Up Question

Why do you think so few people respond to questionnaires dealing with security?	
1	Because we don't know who will have access to identifying information from the survey and we don't want to advertise our vulnerabilities.
2	Some people are reluctant to publicize threats because it shows weakness and vulnerability.
3	Most people think that their security is adequate, but many may not want to admit that they don't understand security.
4	Reluctance to make public security arrangements; difficulty of answering the questions with the options provided.
5	Most do not pay attention to security until they are impacted by the loss of same.
6	You never think about it until it happens.
7	Lack of understanding and denial that there is a problem. Securing computerized data is not understood by many IT professionals. Law firms in the U.S. are historically conservative in changing systems that appear to work and fix something only when it has broken.
8	They either do not want to admit that their own firm has poor security or they have some silly idea that expressing knowledge of security policies somehow infringes on the security of their firm.
9	:-) They either don't know anything about it or they don't care.
10	Too shy to show that their office might be at risk, we always think that we don't do enough to protect our system. Also too afraid to be noticed.
11	For security reasons. Most people wouldn't want to describe the security system they have at home for fear it could help people break in.
12	Because they do not understand the issues
13	Fear, exposure and liability.
14	They don't want to show their ignorance of the issue
15	I don't think it's limited to security issues. But I do think that I hide the most ridiculous things from vendors (the name of my backup vendor; when the tapes go offsite; stuff that doesn't matter) in the name of security. Maybe people don't want to share something that, put together with all the other things, could cause a security breach?
16	People get asked to fill out surveys every day.
17	Fear of disclosure
18	Not enough time to respond to surveys
19	They are hiding from the fact that they are vulnerable.
20	So few people know about it! And it's an emotionally difficult area to talk about when your firm isn't up to standards.
21	It reminds them how their security is lacking in every area and how they are not following proper legal procedures
22	Because they are afraid of the unknown and are embarrassed of their answers.
23	Fear that the information will be used against them. Embarrassment. Ignorance on the subject. Many do not understand security and assume someone is taking care of it.
24	Exposure to media.
25	Because we are all concerned about our security and would not like others to know any vulnerabilities
26	Afraid of public knowledge that will damage the chances for future business and cause loss of current customers.

Why do you think so few people respond to questionnaires dealing with security?	
27	Probably don't want to take the time to respond.
28	Besides the fact it's a difficult (as in intellectually challenging) area, it may be an area no one really believes requires concern -- or expenditures -- until a problem actually surfaces (when the horse is on the way out of the barn). I know I am often accused of being "alarmist" and "going overboard on this stuff" and that likely won't change until (and if) an incident occurs (and if that incident costs money, it will immediately become "why haven't we?").
29	Out of sight, out of mind.
30	Don't want to admit to not having adequate security procedures in place.

Findings

Demographics Analysis

Demographic questions such as level of education, gender, age, and job level were included in the survey instrument. The basic demographic analysis was performed using Microsoft[®] Excel[®]. Table 6 presents this demographic analysis. The gender distribution demonstrated that about two-thirds (66%) of the survey respondents were male and approximately one-third (34%) were female. Most of the respondents (42%) were between the ages of 36 and 45. Over one-half of the respondents (55%) held the title of CIO/Director. More than one-half of the respondents (52%) hold Bachelor degrees, while an additional number of respondents (19%) possess advanced degrees of Master degrees and one holds a law degree (1%).

Table 6. Demographic Data of the Study Respondents

Item	Frequency	Percentage
High School Graduate	7	8%
Paralegal Certificate	0	0%
Bachelor Degree	46	52%
Master Degree	17	19%
Juris Doctorate	1	1%
Ph.D.	0	0%
Prefer not to answer	6	7%

Item	Frequency	Percentage
Other, Please Specify	11	12%
1 Some college		
2 AA		
3 Bachelor with 45 hours towards Master		
4 Community College		
5 Military Technical Academy Graduate		
6 Some college		
7 Associate Degree, Microsoft Certs.		
8 Some college credits, but no degree		
9 Technical College		
10 Network Admin Certificate, MS & Novel Cert		
Female	30	34%
Male	57	66%
<i>Age</i>		
18-25	1	1%
26-35	6	7%
36-45	37	42%
46-55	29	33%
56-65	12	14%
65+	0	0%
Prefer not to answer	3	3%
Associate	0	0%
Partner	1	1%
Chief Information Officer/Director	48	55%
Chief Security Officer/Information Security Officer	1	1%
Privacy/Compliance Officer	0	0%
Project Manager	0	0%
Legal Technology Manager	15	17%
Paralegal/Legal Assistant	0	0%
Legal Secretary	0	0%
Technician	0	0%
Database Programmer	0	0%
Database Coder	0	0%
Network Administrator	11	12%
Other, Please Specify	12	14%
1 Director of Information Technology		
2 IT Director		
3 Systems Administrator		
4 Executive Director		
5 Director		
6 Technology Courseware Developer & Trainer		
7 Staff Development & Training Manager		
8 Information Systems Director		
9 Office Manager/Administrator		
10 Director and Network Manager		
11 Director, Technology		
12 engineer		

Law Firm Demographics

The survey instrument collected law firm demographics such as size of law firm in number of users, size of information technology department, location of law firm offices, country where the law firm was based, functions of the law firm technology-related department, whether the law firm had a designated IT security person or group, and title of the IT security person. This demographic data are presented in Tables 7 through 12.

Table 7 reports on the sizes of the respondents' law firms and the percentages of their law firm users. Close to one-half of the respondents (40%) were from small-sized law firms with fewer than 150 users. One-fourth of the respondents were from large-sized law firms with 251-500 users. Almost one-fifth of the respondents (19%) were from medium-sized law firms with 150-250 users. The remaining 16% of the respondents were from very large-sized law firms with less than 150 users.

Table 7. Size of Law Firm in Number of Users of the Study Respondents

Item	Frequency	Percentage
Small <150 Users	35	40%
Medium 151-250 Users	17	19%
Large 251-500 Users	22	25%
Very Large >500 Users	14	16%

Table 8 presents data on the sizes of the respondents' law firm information technology departments. The majority of the respondents (52%) had IT departments with 2 to 10 people.

Table 8. Size of Law Firm Information Technology Department of the Study Respondents

Item	Frequency	Percentage
1	16	18%
2-10	46	52%
11-24	13	15%
>25	13	15%

Tables 9 and 10 report on the location of the respondent law firm offices and the countries where they are based. The majority of the respondents (88%) were based in the U.S., with 10 percent of the respondents based in Canada, and the balance based in Australian (1%) and Asia (1%). Approximately one-half of the respondents had multiple offices in the U.S. (49%) or one office in the U.S. (32%) as their primary office.

Table 9. Location of Law Firm Offices of the Study Respondents

Item	Frequency	Percentage
One office in the United States	28	32%
One office in the United States as well as international office(s)	1	1%
Multiple offices in the United States	43	49%
Multiple offices in the United States as well as international offices	2	2%
Multiple offices in the United States and one international office	4	5%
One international office in Europe	0	0%
Other, please specify	5	7%
One office in Canada	1	1%
Other, please specify	1	1%
Multiple offices in Canada	1	1%
Other, please specify: Multiple of offices in Canada, one in US,UK & Australia	1	1%
Other, please specify: Australia	2	2%

Table 10. Region Where Law Firm Offices of the Study Respondents Were Based

Item	Frequency	Percentage
United States based law firm	77	88%
European Union based law firm	0	0%
Canadian based law firm	9	10%
Asia Pacific based law firm	1	1%
Latin American based law firm	0	0%
Prefer not to answer	0	0%
Other, please specify: Australia	1	1%

Tables 11 and 12 present data regarding the functions of the law firm technology-related departments and report whether the law firm designated a person or group to handle IT security issues. The majority of the respondents' technology-related departments provided information security services (90%), disaster recovery (89%), information security appliance/software implementation (83%), incident response (80%), and information security policy development (78%). Less than one-half of the respondents' technology-related departments provided Web page design/development (49%) and privacy policy development (44%). Very few law firms (2%) outsource all of these functions. Less than three quarters of the law firm respondents (69%) had one person or a group of people designated to handle security issues.

Table 11. Functions of the Law Firm Technology-related Departments of the Study Respondents

Item	Frequency	Percentage
Information security services	80	91%
Information security policy development	69	78%
Privacy policy development	39	44%
Web page design/development	43	49%
Incident response	71	81%
Disaster recovery	78	89%
Information security appliance/software implementation	73	83%
We outsource all of these functions	2	2%
Do not know	2	2%
Other, please specify: Outsource some of these functions	2	2%

Table 12. Law Firm Designation of Security Personnel of the Study Respondents

Item	Frequency	Percentage
Yes, one person	23	26%
Yes, a group of people	38	43%
No	27	31%
Do not know	0	0%

Table 13 presents data regarding statements the respondents indicated were true for their firm. Over one-half (56%) of the respondents indicated that security falls upon everyone in the IT department in their law firm. Close to one-half (48%) of the respondents stated that an individual is designated to be responsible for information security in their law firm. Almost one-quarter (22%) of the respondents did not have any individual designated as responsible for information security in their law firm. Only seven percent of the respondents indicated their law firm had a separate department responsible for information security.

Table 13. Law Firm Respondents' Designation of Responsibility for Information Security

Item	Frequency	Percentage
There is an individual designated as being responsible for information security in my law firm.	42	48%
There is a separate department in my law firm responsible for information security.	6	7%
Information security falls upon everyone in the information technology department in my law firm.	49	56%
No individual is designated as being responsible for information security in my law firm.	19	22%

Table 14 presents data regarding the privacy and security laws applicable to the law firm respondents, including U.S. laws and international laws. Almost one-half of the respondents did not know whether their law firms were required to comply with these laws, or claimed that their law firms did not have to comply with any of these laws.

Table 14. Privacy and Security Laws Identified by Law Firm Respondents for Compliance

Item	Frequency	Percentage
PIPEDA (The Personal Information Protection and Electronic Document Act)	9	11%
State Data Breach Notification Laws	12	15%
European Union Directive on Data Protection	2	2%
GLBA (Gramm-Leach-Bliley Act)	3	4%
HIPAA (Health Insurance Portability and Accountability Act)	31	38%
FACTA (Fair and Accurate Credit Transactions Act)	1	1%
FCRA (Fair Credit Reporting Act)	2	2%
USA P.A.T.R.I.O.T. Act	12	15%
APEC Privacy Principals (Asia Pacific Economic Cooperation)	3	4%
Australia's Federal Privacy Act	3	4%
Japan's Law Concerning the Protection of Personal Information	0	0%
Do not know	32	39%
Other, Please Specify:		
1 None		
2 Canadian Bar Assoc, Law Societies of BC, AB & YT		
3 None	7	9%
4 Not sure of the rest		
5 PIPA - Personal Information Protection Act		
6 None of these apply to us.		
7 Massachusetts Regulation 17		

Follow-up Questions

This dissertation investigation requested that respondents interested and willing to be contacted to answer follow-up questions via an e-mail message linking to a second Zoomerang survey provide their e-mail addresses. Forty-five respondents agreed to respond to follow-up questions and provided their e-mail addresses. Ten questions were posed to this group in a separate Zoomerang survey from April 2, 2009 through April 15, 2009.

According to Romanosky et al. (2008), the critical characteristic of the U.S. data security breach notification laws are that notice is dependent upon where the consumer *resides* rather than where the business is located. Table 14 shows that only 15% of the respondents indicated that their law firms were required to comply with U.S. data security breach notification laws. However, because at the time of the survey there were 44 states (excluding Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota) and the District of Columbia, Puerto Rico, and the Virgin Islands with security breach notification laws, the author speculated that it was likely that the U.S.-based law firms had one or more clients who resided in a state requiring data security breach notifications. In order to test this speculation, the author asked the 45 respondents who had agreed to a follow-up Zoomerang survey whether they had clients who resided in any of these or territories with data security breach notifications. Table 15 presents data regarding the location of where the respondents' law firm offices were based. Thirty-three of the 34 respondents to the follow-up Zoomerang survey responded that they had clients that resided in one or more states with data security breach notification laws, including four of the five Canadian law firms represented in Table 15. Table 16 presents the mean and standard deviation (Std. D.) for the follow-up questions pertaining to the respondents' understanding of U.S. data breach notification laws. These descriptive statistics were calculated using SPSSTM and included a five-point Likert scale (1=strongly disagree to 5 =strongly agree).

Table 15. Region Where Law Firm Offices of the Follow-up Respondents Were Based

Item	Frequency	Percentage
United States based law firm	29	85%
European Union based law firm	0	0%
Canadian based law firm	5	15%
Asia Pacific based law firm	0	0%
Australian based law firm	0	0%
Prefer not to answer	0	0%
Other, please specify	0	0%

Table 16. U.S. Security Breach Notification Laws

Item	Mean	Std. D.
Aware of notification laws in 44 states (excluding Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota), the District of Columbia, Puerto Rico, and the Virgin Islands that require that in the event personal information (PI) and/or personally identifiable information (PII) is exposed to unauthorized parties, the affected clients be notified.	3.74	1.082
Aware that these U.S. security breach notification laws mandate notification to its state residents of lost, stolen, or compromised unencrypted PI and/or PII through unauthorized access to computerized data, including access by an unauthorized employee.	3.65	1.203
Notification of a security breach of computerized data pursuant to these U.S. security breach notification laws is based on where the resident resides rather than where the data resides.	3.29	.906

Survey Data Analysis

The author collected data to measure the incidence (0 occurrences, 1-5 occurrences, 6-10 occurrences, and >10 occurrences) of breaches (computer virus, hacking incident, unauthorized access, theft of hardware/ software, computer-based fraud, human error, natural disaster, and damage by employees) within the two years preceding the survey along with the severity of the breaches using a five-point Likert scale (1=fairly insignificant to 5 =highly significant). Data were collected using the same questions that Doherty and Fulford (2005) used in their study. Table 17 presents the published results from the Doherty and Fulford study. Table 18 presents the descriptive results of the

author's dissertation survey with regard to incidence of breaches and severity of worst breach. The not applicable (N/A) responses were treated as missing values and not included in the calculation of the mean.

Table 17. Doherty & Fulford Table 2. The Incidence and Severity of Security Breaches

Table 2. The incidence and severity of security breaches

Type of Breach	Incidence of Breaches				Severity of Worst Breach					Mean value
	Approximate number of breaches in last two years				Fairly Insignificant		Highly Significant			
	0	1-5	6-10	> 10	1	2	3	4	5	
Computer virus	6	111	23	77	45	65	47	35	19	2.59
Hacking incident	142	66	1	5	42	21	10	5	4	1.92
Unauthorized access	106	83	13	10	32	42	21	5	7	2.23
Theft of resources	50	123	24	19	43	52	48	20	8	2.38
Computer-based fraud	187	23	0	2	15	10	3	6	2	2.15
Human error	41	85	19	65	32	61	43	23	10	2.48
Natural disaster	160	54	2	1	16	24	9	11	5	2.52
Damage by employees	185	28	0	0	20	8	7	2	2	1.82

Note. Adapted with permission of the Publisher (see Appendix A) from ©2005 *Information Resources Management Journal* article, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," p. 29 by N.F. Doherty and H. Fulford.

Table 18. Law Firms – Incidence and Severity of Security Breaches

Type of Breach	Incidence of Breaches				Severity of Worst Breach					Mean Value	
	Approximate Number of Breaches in Last Two Years				Fairly Insignificant		Highly Significant				
	0	1-5	6-10	>10	1	2	3	4	5	N/A	
Computer virus	26	34	11	15	29	13	11	11	5	18	2.28
Hacking Incident	81	3	0	0	19	1	3	0	0	61	1.30
Unauthorized access	55	24	2	2	23	8	5	6	0	43	1.86
Theft of hardware/software	40	35	7	1	23	9	8	14	1	30	2.29
Computer-based fraud	79	4	0	0	20	3	3	0	0	59	1.35
Human Error	21	46	6	11	34	15	9	11	1	15	2.00
Natural Disaster	73	9	0	0	18	3	2	2	2	57	1.78

Type of Breach	Incidence of Breaches				Severity of Worst Breach						
	Approximate Number of Breaches in Last Two Years				Fairly Insignificant			Highly Significant		Mean Value	
Damage by Employees	78	4	0	0	17	2	3	1	0	61	1.48

Research Questions Answered

This Web-based study consisted of 10 primary research questions. The first five questions were derived from Doherty and Fulford's (2005) research on the relationship between written information security policies and security breaches in an exploratory analysis of U.K. organizations employing more than 250 people. The author converted their hypotheses into research questions for this dissertation investigation in order to discover how law firms compare to the subjects in the Doherty and Fulford study. The additional five research questions in the Web-based survey were designed to investigate whether information security policies impact law firms. The 10 primary research questions investigated in this dissertation investigation included:

1. *Do law firms that have written information security policies have fewer security breach incidents in terms of frequency and severity than those that do not have information security policies (Doherty & Fulford, 2005, p. 25)?*

Table 19 presents the published results from the Doherty and Fulford study. Doherty and Fulford found "no statistically significant associations between the existence of an information security policy and either the incidence or the severity of any of the eight types of security breach." (p. 30). While Doherty and Fulford used a chi-square test to display their results, the author's survey responses for the incidence of breaches did not meet the chi-squared test conditions consisting of all expected counts must be >1 and no more than 20% of expected counts could be <5 (Field, 2009). Additionally, the analysis

of variance (ANOVA) conditions were not met since the variables were ordinal and not quantitative. Because neither a chi-squared test nor an ANOVA test was valid to use in this analysis, a Mann-Whitney U test was determined most appropriate (Dr. P. Curtiss, personal communication, May 14, 2009). Table 20 presents the author's dissertation survey Mann-Whitney U results. Because the p-values are all greater than .05, the results demonstrated no evidence of a statistically significant relationship (Field) between the adoption of the information security policy and the incidence and severity of security breaches.

Table 19. Doherty & Fulford – Table 3 The Relationship Between the Adoption of Information Security Policy and the Incidence and Severity of Security Breaches

Table 3. The relationship between the adoption of InSPy and the incidence and severity of security breaches

Type of Breach	Incidence of Breaches (Chi-Squared Analysis)			Severity of Worst Breach (One-Way ANOVA)			
	<i>Pearson Value</i>	<i>Deg. of Freedom</i>	<i>Two-Sided Prob.</i>	<i>Yes</i>	<i>No</i>	<i>F Ratio</i>	<i>F Prob.</i>
Computer virus	0.730	3	0.878	2.59	2.69	0.215	0.644
Hacking incident	5.733	3	0.111	1.92	1.72	0.422	0.518
Unauthorized access	3.090	3	0.378	2.23	2.00	0.730	0.395
Theft of resources	1.905	3	0.607	2.38	2.51	0.429	0.513
Computer-based fraud	1.892	2	0.300	2.15	2.25	0.036	0.851
Human error	5.388	3	0.144	2.48	2.67	0.743	0.390
Natural disaster	6.469	3	0.089	2.52	2.32	0.361	0.550
Damage by employees	0.003	1	1.000	1.82	2.30	1.210	0.279

Note: A chi-squared test was used to test the association between the four categories of incidence (0, 1-5, 6-10, >10) and the two classes of InSPy existence (yes, no), while ANOVA was used to compare the mean severity of breaches and the two classes of InSPy existence.

Note. Adapted with permission of the Publisher (see Appendix A) from ©2005 *Information Resources Management Journal* article, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," p. 30, by N.F. Doherty and H. Fulford.

Table 20. Law Firms – Relationship Between the Adoption of Information Security Policy and the Incidence and Severity of Security Breaches

Type of Breach	Incidence of Breaches (Mann-Whitney U Test)		Severity of Worst Breach (Mann-Whitney U Test)	
	<i>U Test Value</i>	<i>Two-Sided Prob.</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
Computer virus	658.00	0.275	419.00	0.652
Hacking Incident	702.50	0.864	33.00	0.175
Unauthorized access	594.00	0.211	126.00	0.448
Theft of resources	652.00	0.499	277.00	0.950
Computer-based fraud	703.50	0.808	61.50	0.428
Human Error	664.00	0.502	508.00	0.929
Natural Disaster	668.50	0.554	45.00	0.210
Damage by Employees	636.00	0.186	26.00	0.207

2. *Are law firms that have had information security policies in place for numerous years likely to have fewer computer security breach incidents in terms of both frequency and severity than those that do not have information security policies in place (Doherty & Fulford, 2005, p. 25)?*

Table 21 presents the published results from the Doherty and Fulford study. Doherty and Fulford found “that older policies are associated with less severe breaches. However . . . there is no strong or consistent evidence in support of the hypothesis . . .” (p. 31).

Table 22 presents the Spearman’s Rho correlation coefficient used for the author’s ordinal data collected with regard to the age of the information security policy and the incidence/severity of security breaches. Since the p-values are all greater than .05, the results demonstrated no statistically significant associations (Field, 2009) between the age of information security policies and the incidence and severity of security breaches.

Table 21. Doherty & Fulford – Table 4. Relationship between the Age of Information Security Policy and the Incidence/Severity of Security Breaches

Table 4. Relationship between the age of the InSPy and the incidence/severity of security breaches

Type of Breach	Incidence of Breaches (One-Way ANOVA)						Severity of Worst Breach (Correlation)	
	0	1-5	6-10	>10	F Ratio	F Prob.	Pearson Value	Two-Sided Significance
Computer virus	2.0	3.7	3.0	5.1	2.3	.08	-0.05	0.501
Hacking incident	3.7	4.7	5.0	5.0	.77	.51	-0.05	0.718
Unauthorized access	3.5	3.9	4.5	10.1	6.4	.00**	-0.08	0.443
Theft of resources	4.1	3.7	3.4	7.27	3.7	.01*	-0.20	0.025*
Computer-based fraud	3.9	6.14	-	3.00	2.8	.07	-0.13	0.513
Human error	3.9	3.5	3.7	4.9	1.2	.31	-0.00	0.963
Natural disaster	4.1	3.8	2.8	-	.23	.80	-0.15	0.335
Damage by employees	7.8	8.9	-	-	2.9	.09	-0.19	0.332

*Note: * Result significant at the 5% level; ** Result significant at the 1% level*

Note. Adapted with permission of the Publisher (see Appendix A) from ©2005 *Information Resources Management Journal* article, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," p. 31, by N.F. Doherty and H. Fulford.

Table 22. Law Firms – Relationship Between the Age of Information Security Policy and the Incidence/Severity of Security Breaches

Type of Breach	Incidence of Breaches (Spearman's Rho)		Severity of Worst Breach (Correlation)	
	Correlation Coefficient	Two-Sided Significance	Spearman's Rho Value	Two-Sided Significance
Computer virus	0.14	0.302	-0.01	0.941
Hacking Incident	0.05	0.735	0.09	0.735
Unauthorized access	0.05	0.717	-0.10	0.592
Theft of resources	0.11	0.418	0.13	0.427
Computer-based fraud	0.06	0.670	0.11	0.668
Human Error	0.08	0.582	0.07	0.669
Natural Disaster	-0.14	0.324	-0.09	0.710
Damage by Employees	0.07	0.619	0.16	0.521

3. Do law firms that have updated their information security policies on a regular basis have fewer security breach incidents in terms of frequency and severity than those that have not updated their information security policies (Doherty & Fulford, 2005, p. 26)?

Table 23 presents the published results from the Doherty and Fulford study. Doherty and Fulford found “no statistically significant associations between the frequency with which the InSPy is updated and the incidence and severity of any of the eight types of security breach.” (p. 32). Similar to Doherty and Fulford, the author of this dissertation investigation compressed the categorical scales of how often the information technology security policy was updated (more than every two years, every two years, every year, every six months, less than every six months) to greater than or equal to once a year and at least once a year. Table 24 presents the mean rank for this item. Table 25 presents the author’s dissertation survey Mann-Whitney U results. Since the p-values are all greater than .05, the results demonstrated no statistically significant associations (Field, 2009).

Table 23. Doherty & Fulford – Table 5. Relationship Between the Frequency of Updating the Information Security Policy and the Incidence/Severity of Security Breaches

Table 5. Relationship between the frequency of updating InSPy and the incidence/severity of security breaches

Type of Breach	Incidence of Breaches (Chi-Squared Analysis)			Severity of Worst Breach (One-Way ANOVA)			
	Pearson Value	Degree of Freedom	Two- Sided Prob.	< Once a Year	≥Once a Year	F Ratio	F Prob.
Computer virus	3.157	3	0.368	2.42	2.75	2.71	0.101
Hacking incident	1.679	3	0.642	2.00	1.92	0.065	0.799
Unauthorized access	3.108	3	0.375	2.21	2.25	0.030	0.864
Theft of resources	2.219	3	0.528	2.35	2.42	0.117	0.733
Computer-based fraud	1.098	2	0.577	2.08	2.20	0.052	0.821
Human error	5.253	3	0.154	2.67	2.42	1.467	0.228
Natural disaster	3.237	2	0.198	2.29	2.72	1.450	0.235
Damage by employees	1.198	1	0.274	1.73	1.87	0.087	0.770

Note. Adapted with permission of the Publisher (see Appendix A) from ©2005 *Information Resources Management Journal* article, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," p. 32, by N.F. Doherty and H. Fulford.

Table 24. Law Firms – Relationship Between the Frequency of Updating the Information Security Policy and the Incidence of Security Breaches

Type of Breach	How often is the IT security policy updated?	
	< <i>Once a year</i> <i>Mean Value</i>	≥ <i>Once a year</i> <i>Mean Value</i>
Computer virus	27.27	16.50
Hacking Incident	26.07	25.50
Unauthorized access	25.30	27.00
Theft of resources	23.84	33.33
Computer-based fraud	25.14	24.00
Human Error	25.19	27.75
Natural Disaster	24.36	25.50
Damage by Employees	24.71	27.08

Table 25. Law Firms – Relationship Between the Frequency of Updating the Information Security Policy and the Incidence/Severity of Security Breaches

Type of Breach	Incidence of Breaches (Mann-Whitney U Test)		Severity of Worst Breach (Mann-Whitney U Test)	
	<i>U Test Value</i>	<i>Two-Sided Prob.</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
Computer virus	78.00	0.083	65.50	0.586
Hacking Incident	132.00	0.715	6.50	0.789
Unauthorized access	123.00	0.757	26.00	0.094
Theft of resources	79.00	0.096	49.00	0.170
Computer-based fraud	123.00	0.593	6.00	0.695
Human Error	118.50	0.656	54.00	0.110
Natural Disaster	120.00	0.744	13.00	0.593
Damage by Employees	116.50	0.422	10.50	0.498

***Grouping Variable: How often is the IT security policy updated?**

4. *Are law firms that have an information security policy with a broad scope likely to have fewer security breaches in terms of both frequency and severity than those organizations that do not (Doherty & Fulford, 2005, p. 26)?*

Table 26 presents the published results from the Doherty and Fulford study. Doherty and Fulford found “with regard to the severity of threats, there are no statistically significant associations between number of issues covered by the policy and the severity of security breaches.” (p. 33). Table 27 presents the Spearman’s Rho correlation

coefficient results of this dissertation investigation for the relationship between the range of issues covered by the information security policy and the incidence/severity of security breaches. The results demonstrated a significant but weak relationship. It was found that a significant association exists when the number of issues covered in the information security policies increase, the number of thefts of resources also tends to go up. However, since the p-value is less than .05 the correlation is not very strong because it is greater than .8 or less than -.8 (Field, 2009).

Table 26. Doherty & Fulford – Table 6. Relationship Between the Range of Issues Covered by the Information Security Policy and the Incidence/Severity of Security Breaches

Table 6. Relationship between the range of issues covered by the InSPy and the incidence/severity of security breaches

Type of Breach	Incidence of Breaches (One-Way ANOVA)						Severity of Worst Breach (Correlation)	
	0	1-5	6-10	>10	F Ratio	F Prob.	Pearson Value	Two-Sided Significance
Computer virus	8.0	7.8	7.6	8.4	.79	.49	0.05	0.530
Hacking incident	8.0	7.9	10.0	6.5	.41	.75	-0.04	0.779
Unauthorized access	7.9	8.0	7.9	9.4	.86	.46	0.15	0.169
Theft of resources	7.4	8.0	8.2	9.3	2.4	.10	-0.05	0.536
Computer-based fraud	7.8	9.3	-	5.00	3.4	.04*	0.31	0.122
Human error	8.1	7.9	7.8	8.2	.29	.88	0.02	0.838
Natural disaster	7.9	8.5	3.5	-	3.8	.02*	0.24	0.105
Damage by employees	7.8	8.9	-	-	2.9	.09	0.08	0.678

Note: Result significant at the 5% level

Note. Adapted with permission of the Publisher (see Appendix A) from ©2005 *Information Resources Management Journal* article, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," p. 32, by N.F. Doherty and H. Fulford.

Table 27. Law Firms – Relationship Between the Range of Issues Covered by the Information Security Policy and the Incidence/Severity of Security Breaches

Type of Breach	Incidence of Breaches (Spearman's Rho)		Severity of Worst Breach (Correlation)	
	<i>Correlation Coefficient</i>	<i>Two-Sided Significance</i>	<i>Spearman's Rho Value</i>	<i>Two-Sided Significance</i>
Computer virus	-0.13	0.314	0.05	0.722
Hacking Incident	0.05	0.699	0.00	1.000
Unauthorized access	0.18	0.192	0.01	0.961
Theft of resources	0.38	0.004	-0.18	0.256
Computer-based fraud	0.04	0.783	-0.09	0.721
Human Error	-0.04	0.775	-0.25	0.089
Natural Disaster	0.16	0.260	0.02	0.950
Damage by Employees	0.13	0.359	-0.14	0.559

5. *Are law firms that have adopted a wide variety of best practices likely to have fewer security breaches in terms of both frequency and severity than those organizations that have not (Doherty & Fulford, 2005, p. 26)?*

Table 28 presents the published results from the Doherty and Fulford study. Doherty and Fulford found that “there is a statistical association between the summated success factors and security breaches for two out of the 16 tests conducted. . . . given that only two of the 16 tests were significant, there is insufficient evidence to support hypothesis . . . it must be rejected.” (p. 34). Table 29 presents the Spearman’s Rho correlation coefficient results of this dissertation investigation for the relationship between the range of issues covered by the successful adoption of success factors and the incidence/severity of security breaches. Since the p-values are all greater than .05, the results demonstrate no statistically significant associations (Field, 2009).

Table 28. Doherty & Fulford – One-way ANOVA between the Successful Adoption of Success Factors and the Incidence/Severity of Security Breaches

Table 7. One-way ANOVA between the successful adoption of success factors and the incidence/severity of security breaches

Type of Breach	Incidence of Breaches (One-Way ANOVA)						Severity of Worst Breach (Correlation)	
	0	1-5	6-10	>10	F Ratio	F Prob.	Pearson Value	Two-Sided Significance
Computer virus	3.17	2.95	2.85	2.85	0.42	0.74	0.031	0.699
Hacking incident	2.94	2.93	2.50	1.55	3.05	0.03*	0.120	0.365
Unauthorized access	2.99	2.82	2.76	2.75	1.01	0.39	-0.070	0.529
Theft of resources	2.87	2.89	3.01	2.91	0.40	0.75	-0.149	0.097
Computer-based fraud	2.89	2.87	-	2.40	0.27	0.76	0.305	0.138
Human error	2.98	2.87	3.12	2.81	0.99	0.39	-0.189	0.035*
Natural disaster	2.92	2.82	3.20	-	0.50	0.60	0.171	0.255
Damage by employees	2.91	2.86	-	-	0.09	0.76	-0.088	0.655

Note: * Result significant at the 5% level

Note. Adapted with permission of the Publisher (see Appendix A) from ©2005 *Information Resources Management Journal* article, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," p. 33, by N.F. Doherty and H. Fulford.

Table 29. Law Firms – Spearman's Rho Between the Successful Adoption of Success Factors and the Incidence/Severity of Security Breaches

Type of Breach	Incidence of Breaches (Spearman's Rho)		Severity of Worst Breach (Correlation)	
	Correlation Coefficient	Two-Sided Significance	Spearman's Rho Value	Two-Sided Significance
Computer virus	-0.04	0.796	-0.22	0.131
Hacking Incident	-0.02	0.883	-0.05	0.840
Unauthorized access	0.13	0.321	-0.09	0.614
Theft of resources	0.19	0.165	0.06	0.706
Computer-based fraud	-0.15	0.262	-0.39	0.110
Human Error	0.06	0.638	-0.13	0.394
Natural Disaster	-0.06	0.680	-0.19	0.400
Damage by Employees	0.10	0.459	-0.04	0.876

Table 30 presents the responses and percentages for each of 10 success factors' importance of best practices for the effective implementation of IT security in respondent's law firm(s).

Table 30. Law Firm – Success Factors’ Importance of Best Practices

Item	Not at All Important	Not Very Important	Somewhat Important	Very Important	Extremely Important	N/A
Ensuring security policy reflects business objectives	0	0	10	33	18	0
<i>Percentage:</i>	0%	0%	16%	54%	30%	0%
An approach to implementing security that is consistent with the law firm culture	0	2	7	33	19	0
<i>Percentage:</i>	0%	3%	11%	54%	31%	0%
Visible commitment from management	0	0	4	15	42	0
<i>Percentage:</i>	0%	0%	7%	25%	69%	0%
A good understanding of security risks	0	0	5	21	34	0
<i>Percentage:</i>	0%	0%	8%	35%	57%	0%
A good understanding of security requirements	0	0	6	22	33	0
<i>Percentage:</i>	0%	0%	10%	36%	54%	0%
Effective marketing of security to all law firm employees/ lawyers or other members of the firm	0	1	10	34	16	0
<i>Percentage:</i>	0%	2%	16%	56%	26%	0%
Distribution of guidance on IT security policy to all law firm employees/lawyers or other members of the firm	1	1	10	28	20	0
<i>Percentage:</i>	2%	2%	17%	47%	33%	0%
Providing appropriate training and education to all employees/lawyers or other members of the firm	0	3	11	30	17	0
<i>Percentage:</i>	0%	5%	18%	49%	28%	0%
Comprehensive measurement system for evaluating performance in security management	1	4	25	17	13	0
<i>Percentage:</i>	2%	7%	42%	28%	22%	0%
Provision of feedback system for suggesting policy improvements	2	9	26	19	4	0
<i>Percentage:</i>	3%	15%	43%	32%	7%	0%

Table 31 presents the responses and percentages for each of these 10 success factors (best practices) for the effective adoption of IT security in respondent’s law firm(s).

Table 31. Law Firm – Success Factors’ Adoption of Best Practices

Item	Not at All Successful	Not Very Successful	Somewhat Successful	Very Successful	Extremely Successful	N/A
Ensuring security policy reflects business objectives	1	6	26	19	8	1
<i>Percentage:</i>	2%	10%	43%	31%	13%	2%
An approach to implementing security that is consistent with the law firm culture	1	6	19	25	9	1
<i>Percentage:</i>	2%	10%	31%	41%	15%	2%
Visible commitment from management	3	12	20	16	8	1
<i>Percentage:</i>	5%	20%	33%	27%	13%	2%
A good understanding of security risks	3	3	20	26	8	1
<i>Percentage:</i>	5%	5%	33%	43%	13%	2%
A good understanding of security requirements	2	5	22	23	8	1
<i>Percentage:</i>	3%	8%	36%	38%	13%	2%
Effective marketing of security to all law firm employees/ lawyers or other members of the firm	2	19	26	9	4	1
<i>Percentage:</i>	3%	31%	43%	15%	7%	2%
Distribution of guidance on IT security policy to all law firm employees/lawyers or other members of the firm	1	10	26	15	8	1
<i>Percentage:</i>	2%	16%	43%	25%	13%	2%
Providing appropriate training and education to all employees/lawyers or other members of the firm	3	21	23	10	3	1
<i>Percentage:</i>	5%	34%	38%	16%	5%	2%
Comprehensive measurement system for evaluating performance in security management	8	26	17	5	2	3
<i>Percentage:</i>	13%	43%	28%	8%	3%	5%
Provision of feedback system for suggesting policy improvements	8	25	18	8	0	2
<i>Percentage:</i>	13%	41%	30%	13%	0%	3%

Doherty and Fulford (2005) conducted a Cronbach’s alpha measure of the 10 success factors which was found to be statistically significant with a score of 0.87. Similarly, the author of this dissertation investigation performed a Cronbach’s alpha internal reliability

test of the 10 success factors using SPSSTM. According to Sekran (2003), a Cronbach's alpha of over .60 is considered to be statistically significant with those over .80 to be good reliabilities. Table 32 presents the results of this test. Findings indicated the Cronbach's alpha measure of the 10 success factors of this dissertation investigation to be statistically significant with a score of 0.89.

Table 32. Law Firms – Cronbach Alpha Internal Reliability Test of 10 Success Factors

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.895	0.896	10

Table 33 presents the responses and percentages for whether law firm computers are shut down for inactivity after a defined period. More than one-half (67%) of the respondents indicated law firm computers are not shut down for inactivity after a defined period.

Table 33. Law Firm Computers Shut Down for Inactivity After A Defined Period

Item	Frequency	Percentage
Yes	27	31%
No	59	67%
Do Not Know	2	2%

Table 34 presents the responses and percentages for each security issue covered in IT security policies and/or separate procedures or standards in the respondent's law firm(s). The personal usage of information systems was the highest percentage (63%) in the *policy document only* category, with one-half of law firm respondents reporting a policy document only for Internet access (50%), and just under one-half had a policy document only in regard to violations and breaches (49%). Almost one-fourth of the responses under the *stand-alone procedures or standard only* category were in regard to

contingency planning (23%), while close to one-half of the respondents indicated *policy document and supplementary procedure or standards* were in place for disclosure of information (45%), Internet access (43%), and mobile computing (42%).

Table 34. Law Firm – Security Issues Covered in IT Security Policies and/or Separate Procedures or Standards

Item	Policy Document Only	Stand-Alone Procedure or Standard Only	Policy Document & Supplementary Procedure or Standard
Disclosure of information	21	7	27
<i>Percentage:</i>	35%	12%	45%
System access control	24	12	21
<i>Percentage:</i>	40%	20%	35%
Internet access	30	3	26
<i>Percentage:</i>	50%	5%	43%
Viruses, worms & Trojans	26	10	19
<i>Percentage:</i>	43%	17%	32%
Software development	12	2	7
<i>Percentage:</i>	20%	3%	12%
Contingency planning	18	14	13
<i>Percentage:</i>	30%	23%	22%
Encryption	12	7	9
<i>Percentage:</i>	21%	12%	16%
Mobile computing	16	7	25
<i>Percentage:</i>	27%	12%	42%
Personal usage of Information Systems	37	3	19
<i>Percentage:</i>	63%	5%	32%
Physical security	20	8	21
<i>Percentage:</i>	34%	14%	36%
Violations and breaches	28	5	21
<i>Percentage:</i>	49%	9%	37%

Table 35 presents the responses and percentages for whether IT security policies are approved by respondent's law firm management. More than 90 percent of respondents (93%) indicated law firm management does approve IT security policy documents.

Table 35. Law Firms – IT Security Policy Documents Approved By Management

Item	Frequency	Percentage
Yes	57	93%
No	3	5%
Do Not Know	1	2%

Table 36 presents the responses and percentages for whether law firm IT security policy is communicated with all law firm employees/lawyers or other members of the firm and relevant third party service providers. More than one-third of respondents (33%) only communicated approved IT security policy documents to law firm employees/ lawyers or other members of the firm. Just over one-fourth of respondents (28%) communicated all policies with law firm employees/lawyers/other members and third parties. One-fifth of respondents (20%) indicated only certain policies were communicated, while less than one-fifth of respondents (16%) do not communicate policies to relevant third parties.

Table 36. Communication of Law Firm Approved IT Security Policy Documents

Item	Frequency	Percentage
Yes – all of them are communicated to law firm employees/lawyers or other members of the firm and relevant third party service providers	17	28%
Yes – but not communicated to relevant third party service providers	10	16%
Yes – but only communicated to law firm employees/lawyers or other members of the firm	20	33%
Yes – but only certain ones are communicated	12	20%
No – none of them	0	0%
Do not know	2	3%

Table 37 presents the responses and percentages for whether the law firm IT security policy is published. More than 90 percent of respondents (92%) indicated that their law firm published IT security policy documents.

Table 37. Publication of Law Firm IT Security Policy Documents

Item	Frequency	Percentage
Yes	55	92%
No	4	7%
Do Not Know	1	2%

6. *When under a time deadline to finish an assignment, are law firm employees more likely to by-pass security measures in order to complete the task (Post & Kagan, 2007)?*

Table 38 presents the mean and standard deviation for the scanning or installation of security measures using a five-point Likert scale (1=not at all likely to 5 =extremely likely).

Table 38. Law Firm Employees/Lawyers Under a Time Deadline to Finish an Assignment – Use of Security Measures

Item	Mean	Std. D.
Scan a file for viruses	2.40	1.497
Install security software updates	2.03	1.299
Install a digital certificate	1.94	1.207
Install an ActiveX control from an unknown source	3.25	1.243

Table 39 presents the frequency and percentages with which an employee/lawyer in each respondent's law firm scans a file for viruses if under a time deadline to finish an assignment using a five-point Likert scale (1=not at all likely to 5 =extremely likely). This data are grouped by law firm size (small, medium, large, and very large). The majority of law firms in all four categories indicated that it is *not at all likely* or *not very likely* that employees/lawyers in their law firms would scan a file for viruses when under a time deadline to finish an assignment.

Table 39. Law Firm Employees/Lawyers Under a Time Deadline to Finish an Assignment – Scan a File for Viruses

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Scan a file for viruses								
Not At All Likely	14	40%	10	58%	8	36%	3	22%
Not Very Likely	6	17%	3	18%	9	41%	2	14%
Somewhat Likely	5	14%	3	18%	1	5%	2	14%

	Small		Medium		Large		Very Large	
Very Likely	3	9%	0	0%	2	9%	2	14%
Extremely Likely	7	20%	1	6%	2	9%	5	36%

Table 40 presents the frequency and percentages with which an employee/lawyer in each respondent's law firm installs security software updates if under a time deadline to finish an assignment using a five-point Likert scale (1=not at all likely to 5 =extremely likely). This data are grouped by law firm size (small, medium, large, and very large). The majority of law firms in all four categories indicated that it is *not at all likely* or *not very likely* that employees/lawyers in their law firms would install security software updates when under a time deadline to finish an assignment.

Table 40. Law Firm Employees/Lawyers Under a Time Deadline to Finish an Assignment – Install Security Software Updates

	Small		Medium		Large		Very Large	
Install security software updates	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not At All Likely	14	40%	11	65%	10	45%	7	50%
Not Very Likely	8	23%	3	17%	9	40%	3	22%
Somewhat Likely	7	20%	1	6%	1	5%	0	0%
Very Likely	2	6%	1	6%	1	5%	2	14%
Extremely Likely	4	11%	1	6%	1	5%	2	14%

Table 41 presents the frequency and percentages at which an employee/lawyer in each respondent's law firm installs a digital certificate if under a time deadline to finish an assignment using a five-point Likert scale (1=not at all likely to 5 =extremely likely). This data are grouped by law firm size (small, medium, large, and very large). The majority of law firms in all four categories indicated that it is not at all likely or not very

likely that employees/ lawyers in their law firms would install a digital certificate when under a time deadline to finish an assignment.

Table 41. Law Firm Employees/Lawyers Under a Time Deadline to Finish an Assignment – Install a Digital Certificate

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Install a digital certificate								
Not At All Likely	19	54%	10	59%	9	41%	6	43%
Not Very Likely	8	23%	3	17%	7	32%	4	29%
Somewhat Likely	3	9%	1	6%	3	14%	3	21%
Very Likely	3	9%	2	12%	2	9%	0	0%
Extremely Likely	2	5%	1	6%	1	4%	1	7%

Table 42 presents the frequency and percentages with which an employee/lawyer in each respondent's law firm installs an ActiveX control from an unknown source if under a time deadline to finish an assignment using a five-point Likert scale (1=not at all likely to 5 =extremely likely). This data are grouped by law firm size (small, medium, large, and very large). The majority of law firms in all four categories indicated that it is *very likely* or *extremely likely* that employees/lawyers in their law firms would install an ActiveX control from an unknown source when under a time deadline to finish an assignment.

Table 42. Law Firm Employees/Lawyers Under a Time Deadline to Finish an Assignment – Install An ActiveX Control From An Unknown Source

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Install an ActiveX control from an unknown source								
Not At All Likely	3	9%	3	18%	4	18%	2	14%
Not Very Likely	5	14%	0	0%	3	14%	2	14%

	Small		Medium		Large		Very Large	
Somewhat Likely	9	26%	6	35%	3	14%	5	36%
Very Likely	14	40%	6	35%	6	27%	4	29%
Extremely Likely	4	11%	2	12%	6	27%	1	7%

7. *Are law firm security policies created in response to an information security breach incident (Doherty & Fulford, 2005; Wiant, 2005)?*

Table 43 presents the frequency and percentages of law firms that created written IT security policies in response to an information security breach incident. Only two law firms with written IT security policies created their policies in response to a security breach incident.

Table 43. Law Firm Size in Number of Users and Existence of a Security Policy

Law Firm Size in Number of Users	Does your law firm have written information technology (IT) security policies?			Were your law firm written IT security policies created due to a security incident/breach?		
	Yes	No	Do Not Know	Yes	No	Do Not Know
Small 1-150	21	13	1	0	21	0
<i>Percentage:</i>	61%	38%	1%	0.00%	100%	0.00%
Medium 151-250 Users	10	7	0	1	8	1
<i>Percentage:</i>	59%	41%	0.00%	10%	80%	10%
Large 251-500 Users	19	3	0	1	17	1
<i>Percentage:</i>	86%	14%	0.00%	5%	90%	5%
Very Large >500 Users	11	3	0	0	10	1
<i>Percentage:</i>	79%	21%	0.00%	0.00%	91%	9%

Table 44 presents the results from the Spearman's Rho test on each pair of variables (past and future Internet effect on security breaches) and the perceived need for information security policies using a five-point Likert scale (1=strongly disagree to 5=strongly agree). Since the p-values are less than .05 (Field, 2009), there are significant (p-values = .019, .031, and .034) relationships, but because the correlation

coefficients (p-values = .249, .230, and .227) are all below .500 (Field), the correlations are weak between the Internet's projected future effect on information technology security breaches and the perception that the need for security policies is greater today than it was one, three, and five years ago. There is also a significant (p-value = .029) but weak correlation (p-value = .232) between the Internet's effect on IT security breaches experienced over the past few years and the perception that the need for security policies is greater today than it was three years ago.

Table 44. Law Firms – Spearman's Rho Between the Internet's Effect on Breaches and the Need for Policies

Type of Breach	Over the Past Few Years, Internet Has Greatly Increased the Number of Security Breaches Experienced (Spearman's Rho)		In the Coming Years, the Internet Will Greatly Increase the Risk of IT Security Breaches (Spearman's Rho)	
	<i>Correlation Coefficient</i>	<i>Two-Sided Significance</i>	<i>Correlation Coefficient</i>	<i>Two-Sided Significance</i>
Need for policies – greater today than one year ago	.187	.081	.249	.019
Need for policies – greater today than three years ago	.232	.029	.230	.031
Need for policies – greater today than five years ago	.165	.124	.227	.034

Table 45 presents the responses and percentages for whether the perceived amount of attorney-client and/or work product communications over electronic networks in a respondent's law firm(s) is greater today than it was one, three, and five years ago using a five-point Likert scale (1=strongly disagree to 5 =strongly agree). Over one-half of law firms perceived that attorney-client and/or work product online communications are greater today than one year ago (59%); over three quarters reported greater attorney-client and/or work product online communications today than three years ago (85%); and over 90 percent reported greater attorney-client and/or work product online communications than five years ago (92%).

Table 45. Law Firm – Attorney-Client Work Product Communication Over Electronic Networks

Item	Strongly Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Strongly Agree
The amount of attorney-client work product communication over electronic networks is greater today than it was one year ago.	1	3	7	25	52
<i>Percentage:</i>	1%	3%	8%	28%	59%
The amount of attorney-client work product communication over electronic networks is greater today than it was three years ago.	0	0	0	13	75
<i>Percentage:</i>	0%	0%	0%	15%	85%
The amount of attorney-client work product communication over electronic networks is greater today than it was five years ago.	0	0	0	7	81
<i>Percentage:</i>	0%	0%	0%	8%	92%

8. *Are risk assessments, network vulnerability scans, and/or penetration tests a part of law firms' validation of the intended security policies (Myler & Broadbent, 2006; Verdon, 2006)?*

Table 46 presents the frequency and percentages of security tasks performed by the respondent law firms during the preceding 12 months.

Table 46. Law Firm – Performance of Security Tasks During the Past 12 Months

Item	Not at All	More Than Once a Year	Once a Year	Once a Month	Every Day	Do Not Know
Perform a vulnerability assessment that scanned the law firm networks to identify potential security risks.	34	15	24	8	3	3
<i>Percentage:</i>	39%	17%	28%	9%	3%	3%
Hire an outside consultant to perform a risk assessment to identify the potential threats, probabilities, and impact of threats to the law firm's	58	6	20	1	0	3

Item	Not at All	More Than Once a Year	Once a Year	Once a Month	Every Day	Do Not Know
management controls, operational controls, and technical controls.						
<i>Percentage:</i>	66%	7%	23%	1%	0%	3%
Conduct an in-house risk assessment of security threats performed by the members of the law firm IT department and/or information security department.	38	12	25	9	0	3
<i>Percentage:</i>	44%	14%	29%	10%	0%	3%
Provide employee training sessions on information security awareness and incident reporting.	53	14	15	3	0	2
<i>Percentage:</i>	61%	16%	17%	3%	0%	2%
Use managed security services of a third party.	50	5	7	1	22	2
<i>Percentage:</i>	57%	6%	8%	1%	25%	2%
Encrypt e-mail messages	42	11	2	6	25	2
<i>Percentage:</i>	48%	12%	2%	7%	28%	2%
Encrypt hard drive data	56	6	2	6	14	4
<i>Percentage:</i>	64%	7%	2%	7%	16%	5%
Review the information security policies of the law firm	23	20	36	4	1	3
<i>Percentage:</i>	26%	23%	41%	5%	1%	3%
Revise the information security policies of the law firm	32	15	35	3	0	1
<i>Percentage:</i>	37%	17%	41%	3%	0%	1%

Table 47 presents the results from a Spearman's Rho test on each pair of variables (security tasks and frequency performed) in relationship to the law firm size. The "Do Not Know" responses were treated as missing variables and therefore were not included in the computations (Field, 2009). Since the p-values are less than .05 (Field, 2009), there are significant relationships between a vulnerability assessment (p-value = .005), use of an outside consultant (p-value = .003), encryption of e-mail (p-value = .001),

encryption of hard drive data (p-value < .001), and revision of a law firm's information security policies (p-value = .036). However, because the correlation coefficients are all below .500 (Field), the correlations are weak between a vulnerability assessment (p-value = .302), use of an outside consultant (p-value = .321), encryption of e-mail (p-values = .347), encryption of hard drive data (p-values = .441), and revision of a law firm's information security policies (p-values = .228).

Table 47. Law Firms – Spearman's Rho Between the Law Firm Size and Each Pair of Variables

Security Measures	Law Firm Size (Spearman's Rho)	
	<i>Correlation Coefficient</i>	<i>Two-Sided Significance</i>
Perform a vulnerability assessment that scanned the law firm networks to identify potential security risks.	.302	.005
Hire an outside consultant to perform a risk assessment to identify the potential threats, probabilities, and impact of threats to the law firm's management controls, operational controls, and technical controls.	.321	.003
Conduct an in-house risk assessment of security threats performed by the members of the law firm IT department and/or information security department.	.131	.234
Provide employee training sessions on information security awareness and incident reporting.	.011	.920
Use managed security services of a third party.	.084	.447
Encrypt e-mail messages	.347	.001
Encrypt hard drive data	.441	.000
Review the information security policies of the law firm	.180	.100
Revise the information security policies of the law firm	.228	.036

Table 48 presents the results from a Kruskal-Wallis test used to determine whether there is a difference in the responses from all four size categories of law firms (small, medium, large, and very large) with regard to performing a vulnerability assessment within the past 12 months. The results demonstrated a significant difference between all four categories of law firms (p-value = .043). Table 48 also presents the Mann-Whitney

U p-values that were derived in an effort to identify which law firm sizes differed in regard to performing a vulnerability assessment. There was evidence of a significant difference between the small and large law firms (p-value = .039) and the small and very large law firms (p-value = .015) with regard to performing a vulnerability assessment within the past 12 months.

Table 48. Law Firms Grouped – Law Firm Size and Perform a Vulnerability Assessment

Security Measures	All Four Categories (Small, Medium, Large, and Very Large)	Small and Large (Mann-Whitney U Test)	Small and Large (Mann-Whitney U Test)	Small and Very Large (Mann-Whitney U Test)	Small and Very Large (Mann-Whitney U Test)
	<i>Kruskal-Wallis P-Value</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
Perform a vulnerability assessment that scanned the law firm networks to identify potential security risks.	.043	232.50	.039	126.00	.015

Table 49 presents the frequency and percentages of vulnerability assessments performed within the past 12 months in relationship to law firm size. This data are grouped by law firm size (small, medium, large, and very large). The majority of small law firms (59%) and over one-third of medium law firms (35%) never perform vulnerability assessments. By contrast, almost one-half of large law firms (45%) and one-third of very large law firms (31%) perform a vulnerability assessment once a year. A few large law firms (10%) and very large law firms (8%) performed vulnerability assessments every day.

Table 49. Law Firm Size and Perform a Vulnerability Assessment

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not at All	20	59%	6	35%	5	25%	3	23%
Once a Year	7	20%	4	24%	9	45%	4	31%
More Than Once a Year	5	15%	4	24%	4	20%	2	15%
Once a Month	2	6%	3	17%	0	0%	3	23%
Every Day	0	0%	0	0%	2	10%	1	8%

Table 50 presents the results from a Kruskal-Wallis test used to determine whether there is a difference in the responses from all four size categories of law firms (small, medium, large, and very large) with regard to hiring an outside consultant to perform a risk assessment within the past 12 months. The results demonstrated a significant difference between all four categories of law firms (p-value = .002). Table 50 also presents the Mann-Whitney U p-values that were derived in an effort to identify which law firm sizes differed in regard to hiring an outside consultant to perform a risk assessment within the past 12 months. The author identified a significant difference between the small and very large law firms (p-value = .002) and the medium and very large law firms (p-value = .001) with regard to hiring an outside consultant to perform a risk assessment.

Table 50. Law Firms Grouped – Law Firm Size and Hiring of An Outside Consultant

Security Measures	All Four Categories (Small, Medium, Large, and Very Large)	Small and Very Large (Mann-Whitney U Test)	Small and Very Large (Mann-Whitney U Test)	Medium and Very Large (Mann-Whitney U Test)	Medium and Very Large (Mann-Whitney U Test)
	<i>Kruskal-Wallis P-Value</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
Hire an outside consultant to perform a risk	.002	124.50	.002	45.00	.001

Security Measures	All Four Categories (Small, Medium, Large, and Very Large)	Small and Very Large (Mann-Whitney U Test)	Small and Very Large (Mann-Whitney U Test)	Medium and Very Large (Mann-Whitney U Test)	Medium and Very Large (Mann-Whitney U Test)
	<i>Kruskal-Wallis P-Value</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
assessment to identify the potential threats, probabilities, and impact of threats to the law firm's management controls, operational controls, and technical controls.					

Table 51 presents the frequency and percentages of hiring an outside consultant to perform a risk assessment within the past 12 months in relationship to law firm size. The majority of small (79%), medium (88%), large (54%), and very large (29%) law firms reported not having hired an outside consultant to perform a risk assessment within the past 12 months. One-half of the very large law firms (50%) reported hiring an outside consultant to perform a risk assessment once a year, while small (9%), medium (12%) and large law firms (36%) reported less frequency of hiring an outside consults to perform risk assessments.

Table 51. Law Firm Size and Hiring of An Outside Consultant

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not at All	27	79%	15	88%	12	60%	4	29%
Once a Year	3	9%	2	12%	8	40%	7	50%
More Than Once a Year	4	12%	0	0%	0	0%	2	14%
Once a Month	0	0%	0	0%	0	0%	1	7%
Every Day	0	0%	0	0%	0	0%	0	0%

Table 52 presents the results from a Kruskal-Wallis test used to determine whether there is a difference in the responses from all four size categories of law firms (small, medium, large, and very large) with regard to conducting an in-house risk assessment within the past 12 months. The results demonstrated no significant difference between the responses of all four categories of law firms (p-value = .320). Table 52 also presents the Mann-Whitney U p-values that were derived in an effort to identify which law firm sizes differed in regard to conducting an in-house risk assessment within the past 12 months. The results demonstrated no significant difference between the combination of small with medium law firms or the combination of large with very large law firms (p-value = .225) with regard to conducting an in-house risk assessment within the past 12 months.

Table 52. Law Firms Grouped – Law Firm Size and In-House Risk Assessment

Security Measures	All Four Categories (Small, Medium, Large, and Very Large)	Small/ Medium and Large/ Very Large (Mann-Whitney U Test)	Small/ Medium and Large/ Very Large (Mann- Whitney U Test)
	<i>Kruskal-Wallis P-Value</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
Conduct an in-house risk assessment of security threats performed by the members of the law firm IT department and/or information security department.	.320	717.50	.225

Table 53 presents the frequency and percentages of conducting an in-house risk assessment within the past 12 months in relationship to law firm size. The majority of small (50%), medium (59%), and large law firms (42%) reported not having conducted an in-house risk assessment. One-half of the very large law firms have conducted an in-house risk assessment once a year, with over one-quarter of the very large law firms (29%) performing an in-house risk assessment once a month.

Table 53. Law Firm Size and In-House Risk Assessment

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not at All	17	50%	10	59%	8	42%	3	21%
Once a Year	8	23%	3	17%	7	37%	7	50%
More Than Once a Year	6	18%	2	12%	4	21%	0	0%
Once a Month	3	9%	2	12%	0	0%	4	29%
Every Day	0	0%	0	0%	0	0%	0	0%

Table 54 presents the results from a Kruskal-Wallis test used to determine whether there is a difference in the responses from all four size categories of law firms (small, medium, large, and very large) with regard to providing employee training sessions on information security awareness and incident reporting within the past 12 months. The results demonstrated no significant difference between all four categories of law firms (p -value = .770). Table 54 also presents the Mann-Whitney U p -values that were derived in an effort to identify which law firm sizes differed in regard to providing employee training sessions on information security awareness and incident reporting. The results demonstrated no significant difference between the combination of small with medium law firms or the combination of large with very large law firms (p -value = .867) with regard to providing employee training sessions on information security awareness and incident reporting within the past 12 months.

Table 54. Law Firms Grouped – Law Firm Size and Employee Training

Security Measures	All Four Categories (Small, Medium, Large, and Very Large)	Small/ Medium and Large/ Very Large (Mann-Whitney U Test)	Small/ Medium and Large/ Very Large (Mann- Whitney U Test)
	<i>Kruskal-Wallis P-Value</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
Provide employee training sessions on information security awareness and incident reporting.	.770	842.00	.867

Table 55 presents the frequency and percentages of providing employee training sessions on information security awareness and incident reporting in relationship to the law firm size within the past 12 months. The majority of small (63%), medium (59%), large law firms (70%), and very large law firms (54%) reported not having provided employee training sessions on information security awareness and incident reporting within the past 12 months.

Table 55. Law Firm Size and Employee Training

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not at All	22	63%	10	59%	14	70%	7	54%
Once a Year	5	14%	4	23%	3	15%	3	23%
More Than Once a Year	7	20%	3	18%	3	15%	1	8%
Once a Month	1	3%	0	0%	0	0%	2	15%
Every Day	0	0%	0	0%	0	0%	0	0%

Table 56 presents the results from a Kruskal-Wallis test used to determine whether there is a difference in the responses from all four size categories of law firms (small, medium, large, and very large) with regard to using managed security services of a third party within the past 12 months. The results demonstrated no significant difference between all four categories of law firms (p-value = .094). Table 56 also presents the Mann-Whitney U p-values that were derived in an effort to identify which law firm sizes differed in regard to using managed security services of a third party. There is no evidence of a significant difference between the combination of small with medium law firms or the combination of large with very large law firms (p-value = .524) with regard to using managed security services of a third party within the past 12 months.

Table 56. Law Firms Grouped – Law Firm Size and Third Party Services

Security Measures	All Four Categories (Small, Medium, Large, and Very Large)	Small/ Medium and Large/ Very Large (Mann-Whitney U Test)	Small/ Medium and Large/ Very Large (Mann- Whitney U Test)
	<i>Kruskal-Wallis P-Value</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
Use managed security services of a third party.	.094	812.00	.524

Table 57 presents the frequency and percentages of using managed security services of a third party within the past 12 months in relationship to law firm size. The majority of small (59%), medium (75%), and large law firms (68%), reported not having used managed security services of a third party within the past 12 months. Over one-quarter of small law firms (29%) and almost one-half of very large law firms (43%) reported using managed security services of a third party every day.

Table 57. Law Firm Size and Third Party Services

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not at All	20	59%	12	75%	14	68%	4	29%
Once a Year	2	6%	4	25%	2	9%	3	21%
More Than Once a Year	2	6%	0	0%	2	9%	1	7%
Once a Month	0	0%	0	0%	1	5%	0	0%
Every Day	10	29%	0	0%	2	9%	6	43%

Table 58 presents the results from a Kruskal-Wallis test used to determine whether there is a difference in the responses from all four size categories of law firms (small, medium, large, and very large) with regard to encrypting e-mail messages within the past 12 months. The results demonstrated a significant difference between all four categories of law firms (p-value = .009). Table 58 also presents the Mann-Whitney U p-values that were derived in an effort to identify which law firm sizes differed in regard to who

encrypted e-mail messages. There was evidence of a significant difference between the small and medium (p-value = .018), small and large (p-value = .029), and small and very large (p-value = .001) law firms who encrypt e-mail messages.

Table 58. Law Firms Grouped – Law Firm Size and Encrypt E-mail Messages

Security Measures	All Four Categories (Small, Medium, Large, and Very Large)	Small and Medium (Mann-Whitney U Test)	Small and Medium (Mann-Whitney U Test)	Small and Large (Mann-Whitney U Test)	Small and Large (Mann-Whitney U Test)	Small and Very Large (Mann-Whitney U Test)	Small and Very Large (Mann-Whitney U Test)
	<i>Kruskal-Wallis P-Value</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
Encrypt e-mail messages	.009	185.50	.018	248.00	.029	111.50	.001

Table 59 presents the frequency and percentages of encrypting e-mail messages within the past 12 months in relationship to the law firm size. The majority of small law firms (73%), and over one-third of medium (35%), and large (43 %) law firms, reported never having encrypted e-mail messages within the past 12 months. Small (18%), medium (35%), large (38%), and very large (36%) law firms reported encrypting e-mail messages every day.

Table 59. Law Firm Size and Encrypt E-mail Messages

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not at All	25	73%	6	35%	9	43%	2	14%
Once a Year	0	0%	0	0%	0	0%	2	14%
More Than Once a Year	2	6%	4	24%	3	14%	2	14%
Once a Month	1	3%	1	6%	1	5%	3	22%
Every Day	6	18%	6	35%	8	38%	5	36%

Table 60 presents the results from a Kruskal-Wallis test used to determine whether there is a difference in the responses from all four size categories of law firms (small, medium, large, and very large) with regard to encrypting hard drive data within the past 12 months. There is a significant difference between all four categories of law firms (p-value = .001). Table 60 also presents the Mann-Whitney U p-values that were derived in an effort to identify which law firm sizes differed in regard to encryption of hard drive data. There is a significant difference between the small and large (p-value = .005) and small and very large (p-value < .001) law firms that reportedly encrypt hard drive data.

Table 60. Law Firms Grouped – Law Firm Size and Encrypt Hard Drive Data

Security Measures	All Four Categories (Small, Medium, Large, and Very Large)	Small and Large (Mann-Whitney U Test)	Small and Large (Mann-Whitney U Test)	Small and Very Large (Mann-Whitney U Test)	Small and Very Large (Mann-Whitney U Test)
	<i>Kruskal-Wallis P-Value</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
Encrypt hard drive data	.001	237.50	.005	89.00	.000

Table 61 presents the frequency and percentages of encrypting hard drive data within the past 12 months in relationship to law firm size. The majority of small (88%), medium (63%), and large law firms (57%), reported never encrypting hard drive data within the past 12 months. One-third of large law firms (33%) and more than one-third of very large (39%) law firms repeatedly encrypt hard drive data every day.

Table 61. Law Firm Size and Encrypt Hard Drive Data

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not at All	30	88%	10	63%	12	57%	4	31%
Once a Year	1	3%	0	0%	0	0%	1	7%

	Small		Medium		Large		Very Large	
More Than Once a Year	0	0%	3	19%	2	10%	1	7%
Once a Month	2	6%	2	12%	0	0%	2	16%
Every Day	1	3%	1	6%	7	33	5	39%

Table 62 presents the results from a Kruskal-Wallis test used to determine whether there is a difference in the responses from all four size categories of law firms (small, medium, large, and very large) with regard to reviewing the law firm information security policies within the past 12 months. The results demonstrated no significant difference between all four categories of law firms (p-value = .410). Table 62 also presents the Mann-Whitney U p-values that were derived in an effort to identify which law firm sizes differed in regard to review of the law firm information security policies. There was no evidence of a significant difference between the combination of small with medium law firms or the combination of large with very large law firms (p-value = .145) with regard to reviewing the law firm information security policies within the past 12 months.

Table 62. Law Firms Grouped – Law Firm Size and Review of Information Security Policies

Security Measures	All Four Categories (Small, Medium, Large, and Very Large)	Small/ Medium and Large/ Very Large (Mann-Whitney U Test)	Small/ Medium and Large/ Very Large (Mann-Whitney U Test)
	<i>Kruskal-Wallis P-Value</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
Review the information security policies of the law firm	.410	691.50	.145

Table 63 presents the frequency and percentages of reviewing the law firm information security policies within the past 12 months in relationship to law firm size. Over one-third of small (35%) and over one-third of medium (35%) law firms reported

not having reviewed information security policies within the past 12 months. Small (38%), medium (30%), large (60%), and very large (47%) law firms review information security policies once a year. Small (27%), medium (30%), large (20%), and very large (15%) review information security policies more than once a year.

Table 63. Law Firm Size and Review of Information Security Policies

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not at All	12	35%	6	35%	3	15%	2	15%
Once a Year	13	38%	5	30%	12	60%	6	47%
More Than Once a Year	9	27%	5	30%	4	20%	2	15%
Once a Month	0	0%	1	5%	1	5%	2	15%
Every Day	0	0%	0	0%	0	0%	1	8%

Table 64 presents the results from a Kruskal-Wallis test used to determine whether there is a difference in the responses from the four categories of law firms (small, medium, large, and very large) with regard to revising the information security policies within the past 12 months. The results demonstrated no significant difference between all four categories of law firms (p -value = .219). Table 64 also presents the Mann-Whitney U p -values that were derived in an effort to identify which law firm sizes differed in regard to review of the law firm information security policies. There was no evidence of a significant difference between the combination of small with medium law firms and the combination of large with very large law firms (p -value = .056) with regard to revising the information security policies within the past 12 months.

Table 64. Law Firms Grouped – Law Firm Size and Revise Information Security Policies

Security Measures	All Four Categories (Small, Medium, Large, and Very Large)	Small/ Medium and Large/ Very Large (Mann-Whitney U Test)	Small/ Medium and Large/ Very Large (Mann- Whitney U Test)
	<i>Kruskal-Wallis P-Value</i>	<i>U Test Value</i>	<i>Two-Sided Prob.</i>
Revise the information security policies of the law firm	.219	660.00	.056

Table 65 presents the frequency and percentages with regard to revising the information security policies in relationship to the law firm size within the past 12 months. The majority of small (51%) and medium (47%) law firms reported not having revised the information security policies within the past 12 months. The majority of large (65%) and very large (62%) law firms revise the information security policies once a year.

Table 65. Law Firm Size and Revise Information Security Policies

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not at All	18	51%	8	47%	4	20%	2	15%
Once a Year	10	29%	4	24%	13	65%	8	62%
More Than Once a Year	7	20%	4	24%	3	15%	1	8%
Once a Month	0	0%	1	5%	0	0%	2	15%
Every Day	0	0%	0	0%	0	0%	0	0%

Table 66 presents the frequency and percentages of auditing and enforcing the documented IT security policy in relationship to law firm size. The majority of small (67%) and medium (63%) law firms reported their law firms do not audit and enforce the documented IT security policy. More than one-half of large law firms (59%) and more

than two-thirds of very large (82%) law firms audit and enforce the documented IT security policy.

Table 66. Law Firm Size and Audit and Enforce Documented IT Security Policy

Law Firm Size in Number of Users	Does your law firm audit and enforce the documented IT security policy?	
	Yes	No
Small 1-150	7	14
<i>Percentage:</i>	33%	67%
Medium 151-250 Users	3	5
<i>Percentage:</i>	37%	63%
Large 251-500 Users	10	7
<i>Percentage:</i>	59%	41%
Very Large >500 Users	9	2
<i>Percentage:</i>	82%	18%

Table 67 presents the frequency and percentages with regard to IT security policy audited by an independent third party. The majority of small (95%) and medium (78%) law firms, and over one-third of large (35%) law firms, and over one-fourth of very large (27%) law firms reported never having the IT security policy audited by an independent third party. Small (5%), medium (22%), large (24%), and very large (18%) law firms have the IT security policy audited by an independent third party more than every two years. Large (29%) and very large (18%) law firms have the IT security policy audited by an independent third party every year.

Table 67. Law Firm Size and IT Security Policy Audited By Independent Third Party

	Small		Medium		Large		Very Large	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Never	19	95%	7	78%	6	35%	3	27%
More Than Every 2 Years	1	5%	2	22%	4	24%	2	18%
Every 2 Years	0	0%	0	0%	2	12%	4	37%
Every Year	0	0%	0	0%	5	29%	2	18%
Every 6 Months	0	0%	0	0%	0	0%	0	0%

	Small		Medium		Large		Very Large	
Less Than Every 6 Months	0	0%	0	0%	0	0%	0	0%

Table 68 presents the frequency and percentages with regard to the dissemination of the security policy. The majority of very large (100%), medium (90%) law, and large (84%), and less than one-half of small (48%) law firms reported disseminating the IT security policy to law firm employees/lawyers or other members of the firm on the law firm intranet. The majority of small (81%), medium (80%), large (84%), and over one-half of very large (64%) law firms reported disseminating the IT security policy to law firm employees/lawyers or other members of the firm in the staff handbook.

Table 68. Law Firm Size and Dissemination of the Security Policy

Law Firm Size in Number of Users	Law Firm Intranet		Staff Handbook	
	Checked	Did Not Check	Checked	Did Not Check
Small 1-150	10	11	17	4
<i>Percentage:</i>	48%	52%	81%	19%
Medium 151-250 Users	9	1	8	2
<i>Percentage:</i>	90%	10%	80%	20%
Large 251-500 Users	16	3	16	3
<i>Percentage:</i>	84%	16%	84%	16%
Very Large >500 Users	11	0	7	4
<i>Percentage:</i>	100.0%	0%	64%	36 %

9. *Do larger law firms (more than 251 users) and smaller law firms (less than 250 users) differ in whether they have written information security policies (Gibney & Corham, 2008)?*

Table 69 presents the frequency and percentages with regard to the results from a Chi-Square test on the existence of a security policy in relationship to the law firm size where the four categories of law firms are placed into the combination of small with medium law firms or the combination of large with very large law firms. The “Do Not Know”

responses were treated as missing variables and therefore were not included in the computations (Field, 2009). The results demonstrated significant test results (p -value = .024) indicating that the law firm combination of large with very large law firms tend to have more written information security policies than the combination of small with medium law firms.

Table 69. Law Firm Groups – Law Firm Size and Written Information Security Policy

Law Firm Size in Number of Users	Written Information Security Policy?		Chi-Square <i>Two-Sided Prob.</i>
	Yes	No	
Small 1-150 or Medium 151-250 Users <i>Percentage:</i>	31 61%	20 39%	.024
Large 251-500 or Very Large >500 Users <i>Percentage:</i>	30 83%	6 17%	

Table 70 presents the frequency and percentages with regard to the results from a Fisher's exact test on the existence of a security policy in relationship to the law firm size where *small law firms* is measured against *very large law firms*. The "Do Not Know" responses were treated as missing variables and therefore were not included in the computations (Field, 2009). The results demonstrated no significant difference between small law firms and very large law firms (p -value = .328) with regard to larger law firms having more information security policies than smaller law firms.

Table 70. Small vs. Very Large Law Firm and Written Information Security Policy

Law Firm Size in Number of Users	Written Information Security Policy?		<i>Fisher's Exact Test.</i>
	Yes	No	
Small 1-150 <i>Percentage:</i>	21 62%	13 38%	.328
Very Large >500 Users <i>Percentage:</i>	11 79%	3 21%	

10. Do smaller law firms (less than 250 employees) and larger law firms (more than 251 users) differ in whether written information security policies were due to information security breach incidents (Gibney & Corham, 2008)?

Table 71 presents the frequency and percentages with regard to the results from a Fisher's exact test on information security breach incidents in relationship to the law firm size where the four categories of law firms are placed into the combination of small with medium law firms or the combination of large with very large law firms. The results demonstrated no significant difference between the combination of large with very large law firms and the combination of small with medium law firms (p-value > .999) with regard to information security breaches. An analysis of small law firms and very large law firms was not possible because no one in either group indicated that the law firm's written IT security policies were created due to a security breach incident.

Table 71. Small vs. Very Large Law Firm and Information Security Breach Incidents

Law Firm Size in Number of Users	Information Security Breach Incidents?		<i>Fisher's Exact Test.</i>
	Yes	No	
Small 1-150 or Medium 151-250 Users	1	29	>.999
<i>Percentage:</i>	3%	97%	
Large 251-500 or Very Large >500 Users	1	27	
<i>Percentage:</i>	4%	96%	

Summary of Results

In this chapter, the author provides the in-depth analyses of the findings of all research questions posited in this dissertation investigation. Findings from the Zoomerang survey of law firms are presented in Tables with an explanatory synopsis for each of the

following: law firm demographics, the relationship between information security policy adoption, the age of information security policy, frequency of updating the information security policy, range of issues covered by the information security policy, successful adoption of success factors, adoption of best practices, and incidence by severity of security breaches. Communication of law firm approved IT security policy documents, best practices, and use of security measures were also presented in Tables. Based on the data collected, the author determined that written information security policies were not generally created in response to a security breach incident.

The projected future effect of the Internet on breaches and the perception of the need for policies demonstrated evidence of significant but weak correlations with regard to the perception that the need for security policies is greater today than it was one, three, and five years ago. In conjunction with Internet use, the perception of attorney-client work product communications over electronic networks was that it is greater today than one, three, and five years ago. The dissemination of security policies was primarily through the law firm intranet and/or the staff handbook. This type of dissemination is passive since it requires the law firm employees/lawyers to actively review these without any ramifications if they do not review them on a regular basis (J. Heath Rush, personal communication, June 30, 2009).

Law firm size and the use of audits to enforce documented IT security policies results showed that small and medium law firms typically did not audit and enforce policies whereas large and very large law firms were more inclined to audit and enforce IT security policies. The data demonstrated that law firms of all four size categories of law firms (small, medium, large, and very large) generally did not use an independent third

party to audit the policies. The hiring of an independent third party for audits of IT security policies would be a discretionary budget item (J. Heath Rush, personal communication, June 30, 2009) if not mandated by law. Thus, this finding is not unexpected.

The results also demonstrated the perceived performance of security measures within the past 12 months by each law firm. Evidence of significant, but weak correlations exists between the survey items: *vulnerability assessments, use of an outside consultant, encryption of e-mail, encryption of hard drive data, and revision of a law firm's information security policies*. Those survey items demonstrating no evidence of significant differences were *in-house risk assessments, employee training, use of managed security services, and review of a law firm's information security policies*.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

This chapter articulates the conclusions drawn from the author's analysis of responses to the dissertation research questions. Next, this chapter discusses the implications of these conclusions and reviews the contributions of this research to the body of knowledge relating to information security policies and computer security breach incidents. Recommendations for future research are included. This chapter concludes with a summary of this dissertation investigation.

Conclusions

Doherty and Fulford (2005) performed an exploratory analysis of security policies and security breach incidents that highlighted the need for supplemental research with different target populations. This dissertation investigation advanced the research of Doherty and Fulford by targeting information security policies and security breach incidents in law firms. The goal of this dissertation investigation was to determine whether there is a correlation between the timing of security policy development (proactive versus reactive policy development) and the frequency and severity of security breach incidents in law firms of varying sizes.

The author distributed a survey to ILTA members that was comprised of Doherty and Fulford's (2005) original survey questions, augmented by additional questions designed to elicit information specific to information security policy development and security

breach incident detection in law firms. This dissertation investigation questioned whether law firms are proactive in their information security policy development or reactive to computer security breach incidents. In this dissertation, the author further investigated whether law firms utilize risk assessments, network vulnerability scans, and/or penetration tests to validate the intended security policies and ensure the existence of adequate safeguards from attackers and/or prevention of unauthorized access to law firm confidential information (Myler & Broadbent, 2006). The population for this online survey consisted of law firm IT personnel and others familiar with legal technology in law firms.

The author's first research question was: *Do law firms that have written information security policies have fewer security breach incidents in terms of frequency and severity than those that do not have information security policies (Doherty & Fulford, 2005, p. 25)?* The results demonstrated no evidence of a statistically significant relationship between the existence of a written information security policy and the frequency and severity of security breach incidents within law firms. Likewise, Doherty and Fulford's survey results showed no significant relationship between the existence of a written information security policy and the frequency and severity of security breach incidents generally. This led Doherty and Fulford to reject their working hypothesis that the existence of a written information security policy generally would reduce the frequency and severity of security breach incidents.

It is worth noting that 37% of the survey respondent law firms with written information security policies reported experiencing more than six occurrences of computer viruses within the past two years. While this result may support varying

hypotheses, it appears unlikely to this author that the existence of a written information security policy has the unintended consequence of causing computer viruses. Further research is required to explore whether the increased prevalence of detected security breach incidents may correlate with the extent to which a law firm has incorporated information technology into its practice and/or the law firm's level of sophistication to detect occurrences of computer viruses.

It is also interesting to note that only 4% of the respondents (two law firms with a written information security policy and one law firm without a written information security policy) indicated that they had experienced 1-5 occurrences of external hacking incidents. The remaining 96% of the respondents indicated that they never experienced an external hacking incident.

The author's second research question was: *Are law firms that have had information security policies in place for numerous years likely to have fewer computer security breach incidents in terms of both frequency and severity than those that do not have information security policies in place (Doherty & Fulford, 2005, p. 25)?* The results again demonstrated no evidence of a statistically significant relationship between the length of time that an information security policy was in place in the responding law firms and the frequency and severity of the security breach incidents that the law firms experienced. This finding correlates with Doherty and Fulford's general finding of no strong or consistent evidence of significance as well.

Further research is required to determine the impact of *policy review practices* on the frequency and severity of security breach incidents in law firms with written policies, and/or whether the prevalence of security breach incidents turns less upon the mere

existence of a written policy and more upon the implementation of information security practices without regard to whether those practices are codified into a policy document. Additionally, further research is required to determine if having information security policies in place provides a better response process with appropriate escalation, mitigation, and remediation of threats which in turn assists in the prevention of further attacks (J. Heath Rush, personal communication, June 30, 2009).

The author's third research question was: *Do law firms that have updated their information security policies on a regular basis have fewer security breach incidents in terms of frequency and severity than those that have not updated their information security policies (Doherty & Fulford, 2005, p. 26)?* The results again demonstrated no evidence of a statistically significant relationship between regular policy updates and the frequency and severity of reported/detected security breach incidents. This finding reinforces Doherty and Fulford's findings of no significance.

Among the respondent law firms, the results indicated that when IT security policies were updated less often, incidence of theft increased. The results demonstrated a significant but weak relationship in this regard among the respondent law firms. Further research is required to determine whether this increased incidence of theft is attributable to a failure by law firms to update their information security policies as necessary to cover purchases of new equipment (assets), resulting in heightened risk of theft from unclear parameters regarding the use, storage, and maintenance of such equipment (J. Heath Rush, personal communication, June 30, 2009). Additionally, further research is required to determine whether the existence of regular information security policy updates correlates with the sophistication of prophylactic measures employed by law

firms, resulting in increased detection, not increased incidence, of breaches by firms that regularly update their information security policies.

The author's fourth research question was: *Are law firms that have an information security policy with a broad scope likely to have fewer security breaches in terms of both frequency and severity than those organizations that do not (Doherty & Fulford, 2005, p. 26)?* The results demonstrated a statistically significant but weak relationship between the number of issues addressed in an information security policy and the frequency and severity of reported security breaches. When the number of issues addressed in a responding law firm's information security policy increased, the number of reported thefts of resources also tended to increase. Doherty and Fulford's study found that "the range of issues covered is associated significantly with the incidence of both computer-based fraud and natural disaster. However, an inspection of the data . . . is inconclusive." (p. 33). This dissertation investigation supports Doherty and Fulford's finding of a relationship between the breadth of a law firm's information security policy and the frequency and severity of detected/reported security breaches. And, as with Doherty and Fulford's study, the author's inspection of the data is inconclusive.

The author's fifth research question was: *Are law firms that have adopted a wide variety of best practices likely to have fewer security breaches in terms of both frequency and severity than those organizations that have not (Doherty & Fulford, 2005, p. 26)?* The results demonstrated no evidence of a statistically significant relationship between the *adoption of best practices* and the frequency and severity of perceived/reported security breaches. These results are consistent with Doherty and Fulford's findings of no significance as well. However, further research is required to determine whether the

increased perception and reporting of computer security breaches by law firms that have incorporated best practices into their respective information security departments may correlate with the level of sophistication within such law firms' information security departments. (J. Heath Rush, personal communication, June 30, 2009).

More than 90 percent (93%) of respondents indicated law firm management does approve IT security policy documents. Approximately one-third of respondents (33%) communicated approved IT security policy documents only to law firm employees/lawyers or other members of the firm. Just over one-fourth of respondents (28%) communicated IT security policies to relevant third party service providers in addition to law firm employees/lawyers/other members. One-fifth of respondents (20%) indicated that only certain IT security policy documents were communicated to law firm employees/lawyers, other members of the firm and relevant third party service providers. Less than one-fifth of respondents (16%) reported that they did not communicate IT security policies to relevant third party service providers.

Over two-thirds (67%) of the respondents indicated that law firm computers are not shut down for inactivity after a defined lapse period. Further research is required to determine whether this finding may be attributable to a reluctance by law firm IT and Information Security departments to inconvenience lawyers (J. Heath Rush, personal communication, June 30, 2009) or to inhibit their billable hour capabilities (Bisel, 2007).

When asked to identify the security issues covered in the reporting law firm's IT security policy and/or through separate procedures or standards, the highest percentage of respondent law firms (63%) identified "personal usage of Information Systems" in the *policy document only* category. One-half of law firm respondents (50%) reported a

policy document only for Internet access, and almost one-half (49%) reported a *policy document only* in regard to violations and breaches of security policies. Almost one-fourth of the respondents (23%) identified contingency planning under the *stand-alone procedures or standard only* category, while close to half of the respondents reported that a *policy document and supplementary procedure or standards* were in place for disclosure of information (45%), Internet access (43%), and mobile computing (42%).

The author's sixth research question was: *When under a time deadline to finish an assignment, are law firm employees more likely to by-pass security measures in order to complete the task (Post & Kagan, 2007)?* The results demonstrated that in the majority of law firms, regardless of size, it is *not at all likely* or *not very likely* that people will scan a file for a virus, install security software updates, or install a digital certificate when operating under a time deadline to finish an assignment. Likewise, the majority of law firms in all four size categories reported that it is *very likely* or *extremely likely* that people in their respective law firms would install an ActiveX control from an unknown source when under a time deadline to finish an assignment. Further research is required to determine the prevalence with which people within law firms of various sizes use security measures when not in a hurry to complete a task.

The author's seventh research question was: *Are law firm security policies created in response to an information security breach incident (Doherty & Fulford, 2005; Wiant, 2005)?* The results demonstrated that, generally, written IT security policies in law firms were not created in response to a security breach incident. These findings suggest that information security policies generally are proactively developed by law firms. Further research is required to determine whether law firms respond to media attention to security

breach incidents that happen to others (outside of their respective law firms) by creating information security policies. (J. Heath Rush, personal communication, June 30, 2009). Further research also is needed to determine whether law firms create information security policies in response to media reports of threats (as distinguished from actual security breach incidents) or in response to knowledge of threats among law firm IT personnel.

The results demonstrated a statistically significant but weak correlation between the Internet's past effect on information technology security breaches and the perception that the need for security policies is greater today than it was one, three, and five years ago. The results also demonstrated a statistically significant but weak correlation between the Internet's projected future effect on information technology security breaches and the perception that the need for security policies is greater today than it was three years ago. Over one-half of law firms (59%) perceived that attorney-client and/or work product online communications are greater today than one year ago; over three-quarters (85%) reported that those attorney-client and/or work product online communications are greater today than three years ago; and over ninety percent (92%) reported that those attorney-client and/or work product online communications are greater today than five years ago.

The author's eighth research question was: *Are risk assessments, network vulnerability scans, and/or penetration tests a part of law firms' validation of the intended security policies (Myler & Broadbent, 2006; Verdon, 2006)?* The author identified significant but weak correlations between the following survey items: *vulnerability assessments, use of*

an outside consultant, encryption of e-mail, encryption of hard drives, and revision of a law firm's information security policies.

The results demonstrated a statistically significant difference between all four size categories of law firms (small, medium, large, and very large) with regard to performing a vulnerability assessment within the past 12 months. There is evidence of a significant difference between the small and large law firms and the small and very large law firms with regard to performing a vulnerability assessment within the past 12 months. The majority of small law firms (59%), and over one-third of medium law firms (35%) never perform vulnerability assessments, while almost one-half of large law firms (45%) and approximately one-third of very large law firms (31%) perform a vulnerability assessment once a year. The results demonstrated that a few large law firms (10%) and very large law firms (8%) performed vulnerability assessments every day.

The results demonstrated a significant difference between all four size categories of law firms (small, medium, large, and very large) with regard to hiring an outside consultant to perform a risk assessment within the past 12 months. Specifically, the results demonstrated a significant difference between the small and very large and the medium and very large law firms with regard to hiring an outside consultant to perform a risk assessment. The majority of small (79%), medium (88%), large (54%), and very large (29%) law firms reported not having hired an outside consultant to perform a risk assessment within the past 12 months. One-half of the very large law firms (50%) hired an outside consultant to perform a risk assessment once a year, while small (9%), medium (12%) and large law firms (36%) hired an outside consults to perform risk assessments once a year.

The results demonstrated no significant difference between the responses of all four size categories of law firms (small, medium, large, and very large) with regard to conducting an in-house risk assessment within the past 12 months. Specifically, the results demonstrated no significant difference between the combination of small with medium law firms or the combination of large with very large law firms with regard to conducting an in-house risk assessment within the past 12 months. The majority of small (50%), medium (59%), and large law firms (42%) reported not having conducted an in-house risk assessment. One-half of the very large law firms (50%) have conducted an in-house risk assessment once a year, with over one-fourth of the very large law firms (29%) performing an in-house risk assessment once a month.

The results demonstrated no significant difference between all four size categories of law firms (small, medium, large, and very large) with regard to providing employee training sessions on information security awareness and incident reporting within the past 12 months. Specifically, the results demonstrated no significant difference between the combination of small with medium law firms or the combination of large with very large law firms with regard to providing employee training sessions on information security awareness and incident reporting within the past 12 months. The majority of small (63%), medium (59%), large law firms (70%), and very large law firms (54%) reported not having provided employee training sessions on information security awareness and incident reporting within the past 12 months.

The results demonstrated no significant difference between all four size categories of law firms (small, medium, large, and very large) with regard to using managed security services of a third party within the past 12 months. Specifically, the author identified no

evidence of a significant difference between the combination of small with medium law firms or the combination of large with very large law firms with regard to using managed security services of a third party within the past 12 months. The majority of small (59%), medium (75%), and large law firms (68%), reported not having used managed security services of a third party within the past 12 months. Over one-quarter of small law firms (29%) and approximately one-half of very large law firms (43%) reported using the managed security services of a third party every day.

The results demonstrated no significant difference between all four size categories of law firms (small, medium, large, and very large) with regard to encrypting e-mail messages within the past 12 months. The results did, however, demonstrate a significant difference between the small and medium, small and large, and small and very large law firms that encrypt e-mail messages. Almost three-quarters of small law firms (73%), and over one-third of medium (35%) and large law firms (43%), reported never having encrypted e-mail messages within the past 12 months. The following percentages of law firms reported encrypting e-mail messages every day - small (18%), medium (35%), large (38%), and very large (36%).

The results demonstrated a significant difference between all four size categories of law firms (small, medium, large, and very large) with regard to encrypting hard drive data within the past 12 months. Specifically, the author identified a significant difference between the small and large and small and very large law firms that encrypt hard drive data. The majority of small (88%), medium (63%), and large law firms (57%), reported never encrypting hard drive data within the past 12 months. One-third of large

law firms (33%) and more than one-third of very large (39%) law firms repeatedly encrypt hard drive data every day.

The results demonstrated no significant difference between all four size categories of law firms (small, medium, large, and very large) with regard to reviewing the law firm information security policies within the past 12 months. Specifically, the results demonstrated no significant difference between the combination of small with medium law firms or the combination of large with very large law firms with regard to reviewing the law firm information security policies within the past 12 months. Over one-third of small (35%) and over one-third of medium law firms (35%) reported not having reviewed information security policies within the past 12 months. An annual (once a year) review of information security policies reportedly occurs in over one-third of small law firms (38%), in just under one-third of medium law firms (30%), in almost two-thirds of large law firms (60%), and in just under one-half of very large law firms (47%). Information security policies reportedly are reviewed more than once per year in over one-quarter of small law firms (27%), approximately one-third of medium law firms (30%), and one-fifth of large law firms (20%).

The results demonstrated no significant difference between all four size categories of law firms (small, medium, large, and very large) with regard to revising their respective information security policies within the past 12 months. Specifically, the results demonstrated no significant difference between the combination of small with medium law firms and the combination of large with very large law firms with regard to revising information security policies within the past 12 months. The majority of small law firms (51%), and just under one-half of medium law firms (47%) reported not having revised

their information security policies within the past 12 months. Over two-thirds of large law firms (65%) and just under two-thirds of very large law firms (62%) reported revising their information security policies once each year.

The results demonstrated that approximately two-thirds of small (67%) and medium law firms (63%) do not audit and enforce their respective documented IT security policies. More than one-half of large law firms (59%) and more than three-quarters of very large law firms (82%) reportedly audit and enforce their respective documented IT security policies.

The results demonstrated the overwhelming majority of small law firms (95%), over three-quarters of medium law firms (78%), over one-third of large law firms (35%), and over one-fourth of very large law firms (27%) never had their IT security policy audited by an independent third party. Medium (22%), large (24%), and very large law firms (18%) reported having their respective IT security policies audited by an independent third party more than once every two years. Large (29%) and very large law firms (18%) reported having their respective IT security policies audited by an independent third party every year.

The author's ninth research question was: *Do larger law firms (more than 251 users) and smaller law firms (less than 250 users) differ in whether they have written information security policies (Gibney & Corham, 2008)?* The results demonstrated that the combination of large law firms with very large law firms tended to report more written information security policies than reported by the combination of small law firms with medium law firms. However, the results demonstrated no significant difference

between small law firms and very large law firms with regard to the number of information security policies each has adopted.

The author's 10th research question was: *Do smaller law firms (less than 250 employees) and larger law firms (more than 251 users) differ in whether written information security policies were due to information security breach incidents (Gibney & Corham, 2008)?* The results demonstrated no significant difference between the combination of large with very large law firms and the combination of small with medium law firms with regard to the number of reported information security breaches. An analysis of small law firms and very large law firms was not possible in this regard because no law responding law firm within either size group indicated that its law firm's written IT security policy was created in response to a security breach incident.

Strengths of Study

The number of reported security breach incidents is growing exponentially every year (Greenberg, 2008; Open Source Foundation, 2008; ITRC, 2009). With computer security breaches growing at a rapid pace, this research is of critical significance. Data privacy, identity theft, and data security breach notification laws are becoming more prevalent globally (Gunasekara, 2007; Swire & Bermann, 2007). As a result, security breach incidents must be reported pursuant to these laws (CMS, 2003; Goldberg, 2008; Greenberg, 2008; Greene, 2006; Hildebrand & Savare, 2008; Li & Shaw, 2008; Rey, 2008; Romanosky et al., 2008). Law firm clients are requesting their lawyers to comply with these laws on their behalf when they are hosting the client's sensitive data, including, but not limited to, PII or ePHI (Gunasekara; Wugmeister et al., 2007). The state data security breach notification laws are directly applicable to law firms and

thereby require lawyers to disclose data breach incidents to their clients (J. Heath Rush, personal communication, June 30, 2009). This research provided a basis for analyzing the applicable laws, the manner in which information security best practices are utilized in law firms, and the issues regarding validation of the intended security policies.

There are a number of information security surveys, such as the Computer Security Institute (CSI), Deloitte-Touche Global Security Survey, Australian Computer and Crime and Security Survey, and UK Department of Trade and Industry Security Breach Survey which do not specifically target one population (Pfleeger & Rue, 2008). This survey compared the results from the Doherty and Fulford (2005) survey of large organizations in the U.K. and furthered their research by extension to a different population in the form of law firms. The findings of this dissertation investigation contributed to the body of knowledge by exploring the effectiveness of security policies in reducing the number of computer security breach incidents and distinguished the differences in security measures between small, medium, large, and very large sized law firms.

Limitations

The first limitation of this study was the response rate. ILTA deploys numerous surveys (usually not security-based questions) to its members throughout the year and typically has a survey response rate over 40%. ILTA was chosen to deploy this survey on behalf of the author to its members due to ILTA's historically successful survey return rate; however, only 7.3% of ILTA's members returned valid responses to this survey. This disappointing response rate presents the significant limitation that the answers of those who did not respond to the survey may have been drastically different than those who did respond (Richardson, 2009), inasmuch as, they may have had more computer

security incidents, a higher significance of severity of computer security incidents, and/or less written information security policies.

The second limitation of this study was that only ILTA members received an invitation to participate in this dissertation investigation. As a result, the targeted law firm population included only active members of ILTA. At the time of the author's Web-based survey ILTA had 1,123 members. However, there are numerous law firms in the U.S. that are not ILTA members. Non-ILTA members may have responded quite differently to this survey. Additionally, this survey was only a snapshot in time. Therefore, generalizing the results of this study to all law firms should be done cautiously.

A third limitation of this dissertation investigation was that it can be difficult to obtain the level of trust required to elicit candid responses from individuals to a security survey. The respondents who completed this survey may represent law firms that support active information security initiatives and have diminished fears of responding to a security survey because they understand security concepts. Those law firms that did not respond may have chosen not to do so out of fear that their survey response would disclose unreported security breaches or vulnerabilities in their law firm's information security policies or practices.

Implications

The research findings of this dissertation investigation provide valuable insights into the information security policies, computer security breach incidents, and security measures that exist in law firms of various sizes throughout the world. The implications of this dissertation investigation to information security policies and practices are

significant. The body of knowledge pertaining to information security policies and practices has been expanded by this dissertation investigation in critical respects beyond the research of Doherty and Fulford (2005) and Wiant (2005).

The first implication of this dissertation investigation relates to a discovery of whether security policies created proactively aid in preventing security breach incidents and how security measures are utilized by law firms. This investigation furthers the research of Doherty and Fulford (2005), as well as Wiant (2005) in smaller sized organizations with different populations, policies, and compliance issues. In this dissertation investigation, the nature of the organizations studied has been expanded beyond hospitals (Wiant) to include an analysis of information security policies in law firms, which have different regulatory compliance issues, interdependence on technological connections, and populations of employees and clients. Also, in the author's research the size of the organizations studied was expanded beyond large organizations employing more than 250 people (Doherty & Fulford,) to include smaller sized law firms including anywhere from 1 up to 250 computer users. Additionally, the geographic boundaries of the investigation have been extended beyond Europe to include the U.S., Canada, Australia, and the Asia Pacific.

The second implication of this dissertation investigation is associated with a confirmation of the findings of the Doherty and Fulford (2005) survey showing that information security policies are proactively developed. Dissimilar findings of this dissertation investigation revealed that respondent law firms with written information security policies reported experiencing more occurrences of computer viruses within the past two years. These findings may imply either that the existence of a written

information security policy has the unintended consequence of causing computer viruses which would seem highly unlikely or, more likely, that the existence of a written information security policy correlates with a law firm's sophistication to detect occurrences of computer viruses, thus explaining the increased prevalence of reported computer viruses among law firms with written information security policies.

The third implication of this dissertation investigation concerns the reporting of external hacking. This research verifies the conclusions of Sveen et al. (2007) that security breach incidents are under reported. Given the prevalence of external hacking incidents (Richardson, 2009), the author's finding of virtually non-existent reporting of external hacking incidents may indicate one or more of the following: (1) that the responding law firms had not detected, or otherwise were unaware of, attempted hacking incidents (inadvertent under-reporting); (2) that the responding law firms were reluctant to disclose their potential vulnerability to information security breaches by acknowledging incidents of external hacking (intentional under-reporting); and/or (3) that, even in the absence of a written information security policy, the majority of respondents had implemented appropriate safeguards to prevent against external hacking. According to Richardson, based on the propensity of cyber criminals to attack systems, and the fact that no firewall or anti-virus stops every attack, it is difficult to have perfect security safeguards in place to prevent all external hacking attempts.

The fourth implication of this dissertation investigation was the finding that when information security policies were updated less often, theft of resources went up. This indicates the importance of regular reviews of the information security policies to

incorporate the purchase of new equipment (assets) and to provide guidance for employees with regard to how they should protect assets that change within the law firm.

Recommendations

In addition to the further research previously outlined, additional research is recommended in this evolving area. The first research study that might be developed from this dissertation investigation would be to conduct research to find how other legal-related industries, such as corporations and/or application service providers (ASPs) for litigation support services, compare in both response rate and findings to the Doherty and Fulford (2005) exploratory analysis and this dissertation investigation. For example, a survey of corporate legal departments' responses with regard to security could be compared and contrasted to law firms and would contribute to the information security field in revealing whether security is viewed differently in corporate legal departments. Additionally, this model could be used to survey ASPs specializing in delivery of electronically stored information (ESI) document collections for law firms and corporate legal departments to measure whether their views of security policies and computer security breach incidents are similar to law firms.

A second research study could be developed to discover how to entice respondents to reveal security issues within their organization without fear. There is a paradox with reporting security incidents wherein *you do not know what you do not know* and thus under report security breach incidents. Those law firms that outsource their network perimeter activities may not be aware of their third party provider's efforts in regard to protecting against hacking incidents and may not be aware of the attempts against their law firm (J. Heath Rush, personal communication, June 30, 2009).

A third research study could include whether information security policies are developed out of fear based on the media attention given to breaches that happen to other companies. Further research is necessary to determine whether the incorporation of best practices in a law firm's information security department correlates with the sophistication level of that law firm's information security department, and might correspondingly explain the increased perception and reporting of security breaches by law firms that adopt best practices (J. Heath Rush, personal communication, June 30, 2009).

A fourth research study could address the different law firm practice areas and whether IT security is more prevalent and/or relevant in one area over another. Due to the nature of intellectual property law firms wherein trade secrets and patent applications contain highly sensitive data, there may be a more urgent need for information security safeguards and best practices than at a law firm that does not host such highly sensitive data. Additionally, this research study could also examine the differences between a more recently created law firm (within the last 10 years) and a more established law firm (in existence more than 10 years) to determine if there is a cultural difference in the technology utilized and whether as a consequence there are less information security data breaches.

The emergence and pervasiveness of social networking sites presents additional security issues with regard to securing the network of any organization. Thus, a fifth research study could examine the effects of social networking sites on information security policy development and its frequency and severity of detected/reported security breaches, and whether security measures/controls assist with the monitoring and

detection of data leakage of the organization's confidential data on these social networking sites.

Summary

In this dissertation investigation, the author examined the problem of whether information security policies assist with preventing unauthorized parties from accessing confidential and sensitive information. The author further investigated the exploratory analysis study of Doherty and Fulford (2005) in this dissertation investigation to determine whether security policies aid in abating security breach incidents against law firm data and networks. The author furthered the Doherty and Fulford study by identifying whether information security policies were developed in response to computer security breach incidents or whether concern for computer security breaches prompted the development and implementation of information security policies. Thus, this dissertation investigation posited questions relative to whether information security policies, computer security breach incidents, and security measures are utilized to safeguard law firm data.

The goal of this dissertation investigation was to determine whether law firms are proactive in their security policy development or reactive to security breach incidents. In this dissertation investigation, the author investigated whether law firms utilize risk assessments, network vulnerability scans, and/or penetration tests to validate the intended security policies and ensure the existence of adequate safeguards from attackers and/or prevention of unauthorized access to law firm confidential information (Myler & Broadbent).

The survey questions regarding security threats, information security policies, and successful implementation of information security policies were adopted from the original survey instrument received from Doherty and Fulford (2005). Additional questions posited by the author included self-efficacy issues, applicable privacy laws, management approval and communication of security policies, and utilization of risk assessments and other security measures in law firms (Post & Kagan, 2007; Myler & Broadbent, 2006; Verdon, 2006). This dissertation investigation posited the following 10 specific research questions with the first five questions derived from Doherty and Fulford's research. The additional five research questions in the Web-based survey were designed to investigate how information security policies impact law firms. The 10 primary questions investigated in this dissertation investigation included:

1. Do law firms that have written information security policies have fewer security breach incidents in terms of frequency and severity than those that do not have information security policies (Doherty & Fulford, 2005, p. 25)?
2. Are law firms that have had information security policies in place for numerous years likely to have fewer computer security breach incidents in terms of both frequency and severity than those that do not have information security policies in place (Doherty & Fulford, 2005, p. 25)?
3. Do law firms that have updated their information security policies on a regular basis have fewer security breach incidents in terms of frequency and severity than those that have not updated their information security policies (Doherty & Fulford, 2005, p. 26)?

4. Are law firms that have an information security policy with a broad scope likely to have fewer security breaches in terms of both frequency and severity than those organizations that do not (Doherty & Fulford, 2005, p. 26)?
5. Are law firms that have adopted a wide variety of best practices likely to have fewer security breaches in terms of both frequency and severity than those organizations that have not (Doherty & Fulford, 2005, p. 26)?
6. When under a time deadline to finish an assignment, are law firm employees more likely to by-pass security measures in order to complete the task (Post & Kagan, 2007)?
7. Are law firm security policies created in response to an information security breach incident (Doherty & Fulford, 2005; Wiant, 2005)?
8. Are risk assessments, network vulnerability scans, and/or penetration tests a part of law firms' validation of the intended security policies (Myler & Broadbent, 2006; Verdon, 2006)?
9. Do larger law firms (more than 251 users) and smaller law firms (less than 250 users) differ in whether they have written information security policies (Gibney & Corham, 2008)?
10. Do smaller law firms (less than 250 employees) and larger law firms (more than 251 users) differ in whether written information security policies were due to information security breach incidents (Gibney & Corham, 2008)?

In this dissertation investigation, the author collected data from law firm IT personnel by utilizing Zoomerang, a Web survey tool. Global law firm IT members of ILTA were surveyed with 1,123 invitations sent out to the ILTA membership by the ILTA Executive

Director, Randi Mayes. Information was collected based on a Web-based questionnaire with multi-choice questions, demographic questions, and Likert-scale questions.

Based on the outcomes from this investigation, the author identified a series of findings and implications:

- The results demonstrated in general that written IT security policies in law firms were not created in response to a security breach incident. These findings suggest that information security policies are proactively developed by law firms.
- The author identified a significant but weak relationship between the number of issues addressed in an information security policy and the frequency and severity of reported security breaches. When the number of issues addressed in an information security policy increased, the number of reported thefts of resources also tended to increase.
- There was evidence of a significant but weak correlation between the Internet's past effect on information technology security breaches and the perception that the need for security policies is greater today than it was one, three, and five years ago. The results also demonstrated a significant but weak correlation between the Internet's projected future effect on IT security breaches and the perception that the need for information security policies is greater today than it was three years ago.
- The results demonstrated in general the grouping of large and very large law firms typically have more written information security policies than the grouping of small and medium law firms. However, there is not a significant difference

between small law firms and very large law firms with regard to larger law firms having more information security policies than smaller law firms.

- The author determined that investigation findings did not demonstrate a significant difference in security breach incursions between the grouping of large and very large law firms and the grouping of small and medium law firms. The author was unable to conduct an analysis of small law firms and very large law firms because no one in either group responded that their law firm's written IT security policies were developed in response to a security breach incident.
- The results demonstrated a significant difference between the small and large law firms and the small and very large firms with regard to performing a vulnerability assessment, since small law firms rarely performed *vulnerability assessments* while large and very large law firms performed them on a regular basis.
- The majority of small, medium, and large law firms overall rarely *hired outside consultants to perform risk assessments* or *conducted an in-house risk assessment* within the past 12 months, while respondents from one-half (50%) of the very large law firms indicated they hired an outside consultant once a year and conducted in-house risk assessments once a year. In addition, approximately one-quarter of very large law firm respondents (29%) conduct in-house risk assessments once a month.
- The majority of all four size categories of law firms (small, medium, large, and very large) reported not having provided *employee IS training sessions* on information security awareness and incident reporting within the past 12 months. These findings demonstrate the importance of fostering a security awareness

culture annually to address human errors and insider threats (Chen et al., 2006; Gupta & Hammond, 2005; Kim, 2005; Rotvold, 2008).

- The author identified a significant difference between the small and medium, small and large, small and very large law firms in terms of *encryption of e-mail messages*. Small law firms reported using e-mail encryption technologies for e-mail and hard drive data less frequently than medium, large, and very large law firms. While this is not a surprising finding given the financial constraints of small law firms, it does provide insight for legislators to apply when they consider passing laws mandating that all e-mail messages and hard drives containing PII be encrypted (Worthen, 2008).
- The majority of small and medium law firms reported not having *revised the information security policies* within the past 12 months, while large and very large law firms revise them once a year.

Appendix A

Permissions

Letter of Permission from Neil F. Doherty for Use of Original Survey Instrument

----- Original Message -----

Subject: RE: Do Information Security Policies Reduce the Incidence of Security Breaches

Date: Mon, 08 Dec 2008 14:19:33 +0000

From: N.F.Doherty@lboro.ac.uk N.F.Doherty@lboro.ac.uk

Organization: Loughborough University

To: Faith Heikkila heikkila@nova.edu

Hi Faith

You are welcome to incorporate my study into your dissertation survey.

Very best of luck,

Neil

Letter of Permission from State Legislatures Magazine

Subject:RE: Right to Know Graphics
Date: Tue, 09 Dec 2008 11:06:51 -0700
From: Magazine <magazine@ncsl.org>
To: 'Faith Heikkila' <heikkila@nova.edu>

Ms. Heikkila

I've asked our designer to send those to you. **The credit that should appear with the graphics is ©National Conference of State Legislatures.**

Ed Smith

Subject:RE: Right to Know Graphics
Date: Mon, 08 Dec 2008 15:51:21 -0700
From: Magazine <magazine@ncsl.org>
To: 'Faith Heikkila' <heikkila@nova.edu>

Ms. Heikkila

If you are unable to pay the fee **we can waive it for onetime use in your dissertation.** If you do decide to purchase them, you can send us a check.

So you'd like to use the pie chart and the 50-state map? If those are the ones you need, I can get them from our designer.

Ed Smith

Subject:RE: Right to Know Graphics
Date: Mon, 08 Dec 2008 09:13:21 -0700
From: Magazine <magazine@ncsl.org>
To: 'Faith Heikkila' <heikkila@nova.edu>

Ms. Heikkila

We can provide you with permission to reprint the graphics. Our usual fee in this situation is \$50 per item.

Do you need them in some form other than what appears on the website?

Ed Smith

Letter of Permission from Open Security Foundation

----- Original Message -----

Subject:Re: Open Source Foundation Graphics

Date:Sun, 07 Dec 2008 19:32:36 +0000 (UTC)

From:lyger <lyger@attrition.org>

To:Faith Heikkila <heikkila@nova.edu>

CC:curators@datalossdb.org

References:<493BF334.1020802@nova.edu>

Hi Faith,

Thanks for asking. **Since your dissertation is for educational (and non-profit) purposes, please feel free to use the graphics as you see fit.**

Assuming you are obtaining these from <http://datalossdb.org/statistics> - you can right-click on the graphics of your choice and choose the "Save Image As..." selection. That would be much easier than us sending the images to you via an email attachment.

For suitable credit, if you could add the following below the graphics, it would be appreciated:

"Graphics Used With Permission Courtesy DataLossDB.org - Copyright 2008, Open Security Foundation"

Any questions or comments, please let us know. Best of luck with your dissertation!

Thanks,

Kelly Todd
CCO / Secretary, Open Security Foundation

Letter of Permission from IGI Global for Use of Tables

Subject: PERMISSION: Do Information Security Policies Reduce the Incidence of Security Breaches
Date: Tue, 28 Apr 2009 12:45:30 -0400
From: Jan Travers jtravers@igi-global.com
To: heikkila@nova.edu
References: <014201c9c789\$676b44e0\$3641cca0\$@org>

Dear Faith Heikkila

Your request to use IGI Global copyrighted materials has been forwarded to me for response. For your future reference, please know that permissions to use any materials that carry the IGI Global copyright are the sole property of the publisher and only IGI can grant this permission, therefore it is unnecessary for you to gain the individual author's permissions. IGI Global will grant you the permission to use the tables as requested. Please be sure to label the tables with the citation of where they originally appear and also include the words, "Used with permission of the Publisher."

Thanks, and good luck with your thesis.

Jan Travers
Vice President

(Ms) Jan Travers
Vice President

IGI Global - Disseminator of Knowledge Since 1988
701 E Chocolate Avenue
Hershey Pennsylvania 17033-1240, USA
Tel: 717.533-8845 x112; Fax: 717.533-8661
E-mail: jtravers@igi-global.com
www.igi-global.com

InfoSci-On-Demand allows you to SEARCH thousands of research articles on cutting-edge topics in computer science and IT management then INSTANTLY purchase full-text PDFs of documents you want to download on a pay-per-view basis! Visit www.infosci-on-demand.com for more information. Institutions can also apply for an account with IGI Global making it easier to shop—no credit card needed! To apply now, visit http://www.igi-global.com/forms/igi_credit_application.pdf for the Credit Application.

=====
The information contained in this communication may be confidential, is intended only for the use of the recipient named above, and may be legally privileged. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please re-send this communication to the sender and delete the original message and any copy of it from your computer system. Thank you.

Appendix B

List of Acronyms

Abbreviation/Acronym	Definition
ABA	American Bar Association
ACC	Account Information – Financial
ANOVA	Analysis of Variance
APEC	Asia Pacific Economic Cooperation
ARRA	American Recovery and Reinvestment Act of 2009
ASPs	Application Service Providers
Biz	Business
Board	Federal Reserve System
CAN	Candidate Numbers
CCN	Credit Card Numbers
CDs	Compact Discs
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CMR	Code of Massachusetts Regulations
CoBIT	Control Objectives for Information and Related Technology
COSO	The Committee of Sponsoring Organizations of the Treadway Commission
CSI	Computer Security Institute
CSO	Chief Security Officer
CVEs	Common Vulnerabilities and Exposures
DOB	Date of Birth
Edu	Education
EHRs	Electronic Health Records
e-library	Electronic Library
EMA	E-mail Address
ePHI	Electronic Protected Health Information
ESI	Electronically Stored Information
EU	European Union
FACTA	Fair and Accurate Credit Transaction Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FIN	Financial
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
Gov	Government

Abbreviation/Acronym	Definition
GVSU	Grand Valley State University
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance and Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
HTML	Hypertext Markup Language
IDSs	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IIS®	Microsoft® Internet Information Server
ILTA	International Legal Technology Association
IPSs	Intrusion Protection Systems
IRB	Institutional Review Board
IS	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
IT	Information Technology
ITRC	Identity Theft Resource Center
M.G.L.	Massachusetts General Law
Med	Medical
MISC	Miscellaneous
NAA	Names and Addresses
NCUA	National Credit Union Association
NIST	National Institute of Standards and Technology
NRS	Nevada Revised Statutes
NSU	Nova Southeastern University
OCC	Office of the Comptroller of the Currency
OECD	Organization for Economic Cooperation and Development
PCI DSS	Payment Card Industry Data Security Standards
PDA	Personal Digital Assistant
PDF	Portable Document Format
PHI	Protected Health Information
PII	Personally Identifiable Information
PIPEDA	Personal Information Protection and Electronic Documents Act
SB 1386	California Senate Bill 1386
SCC	Statistical Consulting Center
SOX	Sarbanes-Oxley Act
SPSS™	Statistical Package for the Social Sciences
SSN	Social Security Number
U.K.	United Kingdom
U.S.	United States

Abbreviation/Acronym	Definition
U.S. – CERT	United States Computer Emergency Response Team
USB	Universal Serial Bus
WEP	Wired Equivalent Privacy

Appendix C

IRB Approval



NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: Faith Heikkila
From: James Cannady, Ph.D.
Institutional Review Board


Signature

Date: April 15, 2008

Re: *Secure Remote Access for the Sharing of Documents and Database Content In Law Firms by Multilevel Users*

IRB Approval Number: cannady04150801

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE REACTIONS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2085 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File
Office of Grants and Contracts (if study is funded)

IRB Amendment Approval

File Details

<http://web.scis.nova.edu/studentdts/condetails.cfm?pid=26186&pnum=7...>

:: [Print Preview](#) :: [Close Window](#) ::

Post No. 78

Author: lingwang

Date/Time: January 7, 2009 11:17 AM

Subject: Approved

Comment:

Faith,

Everything now looks good! I have also received the amendment form with both your and Dr. Littman's signatures.

The amendment to the research protocol is hereof officially approved.

Ling

Appendix D



December 10, 2008

Faith M. Heikkila
6259 Shugarbush Trail
Kalamazoo, MI 49009

Re: ILTA Distribution of Faith M. Heikkila
Dissertation Research Questionnaire

Dear Faith:

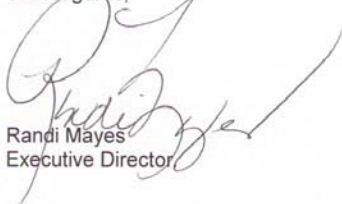
Please accept this letter as my acknowledgement of our agreement to provide ILTA resources in order to facilitate the deployment of your survey as part of your dissertation research.

I am outlining those specific points which we discussed and to which I agreed:

1. ILTA will assist with the distribution of the link to the researcher's Zoomerang survey to its members making sure that only one questionnaire is sent to each law firm, despite multiple offices across the country or globally. After the initial introduction by ILTA with the Zoomerang link, reminder notices will be distributed by ILTA pursuant to their regular schedule of reminders typically sent for other ILTA surveys.
2. The anonymity of the responses will be protected since the researcher will be the only one to receive and review the results of the respondents from ILTA. Also, the responses will not be associated with any identifiable ILTA member e-mail address since it is being deployed as a Web page link and not sent directly from Zoomerang.
3. The questionnaire consists of 35 questions with 12 of them law firm size and demographic questions.
4. Upon approval of the dissertation final report, the researcher will publish the results in an ILTA publication appropriate to the topic.

I am excited to work with you on this project, and I think the responses from the ILTA membership will be a big boon to your dissertation.

With regards,



Randi Mayes
Executive Director

Appendix E

Survey Instrument to ILTA Members



Impact of Information Security Policies on Computer Security Breach Incidents in Law Firms Study

The series of questions in the following four sections are designed to provide information on the impact of information security policies on computer security breach incidents in law firms. The four sections included:

- Section 1: Law firm Information
- Section 2: Security Breach Information
- Section 3: Information Security Policies
- Section 4: Demographic Questions

I appreciate your willingness to participate in this study. Participation in this study is entirely voluntary, with no known risks and no payment provided. Please be advised that all responses were held in strict confidence. Your name will not be linked to your responses. Your name will also not be used in the reporting of information in publications or conference presentations. Only cumulative results were analyzed and placed into my dissertation report. None of the completed questionnaires were reviewed by anyone other than me.

Please provide the response that best describes your knowledge for each question. Results of this survey were published on the International Legal Technology Association (ILTA) Website.

Section 1: Law Firm Information

1. Please indicate the size of your law firm in number of users. Please check only one response.

Law Firm Size	Number of Users	Please check only one response
Small	<151 Users	_____
Medium	151-250 Users	_____
Large	251-500 Users	_____
Very Large	>500 Users	_____

2. Please indicate the size of your law firm information technology department. Please check only one response.

Law Firm IT Dept. Size	Please check only one response
1	_____
2-10	_____
11-25	_____
>25	_____

3. Which of the following most accurately describes the location(s) of your firm's offices? Please check only one response.

Location Description	Please check only one response
One office in the United States	_____
One office in the United States as well as international office(s)	_____
Multiple offices in the United States	_____
Multiple offices in the United States as well as international offices	_____
Multiple offices in the United States and one international office	_____
One international office in Europe	_____

4. Which of the following best describes your law firm? Please check only one response.

Law Firm Description	Please check only one response
United States based law firm	_____
European Union based law firm	_____
Canadian based law firm	_____
Asia Pacific based law firm	_____
Latin American based law firm	_____
Other. Please specify: _____	_____
Prefer not to answer	_____

5. Which of the following information security functions does your law firm technology-related department(s) provide? Please check all that apply.

Information Security Functions	Please check all that apply
Information security services	_____
Information security policy development	_____
Privacy policy development	_____
Web page design/development	_____
Incident response	_____
Disaster recovery	_____
Information security appliance/software implementation	_____
We outsource all of these functions	_____
Other. Please specify: _____	_____
Do not know	_____

6. Does your law firm have a designated person or a group of people who handle security issues? Please check only one response.

Designated Security Person	Please check only one response
Yes, one person	_____
Yes, a group of people	_____
No	_____
Do not know	_____

If **no** or **do not know**, please skip to question 8.

7. If yes, what is their title? Please check only one response.

Title	Please check only one response
Chief Security Officer (CSO)	_____
Chief Information Security Officer (CISO)	_____
Information System Security Officer (ISSO)	_____
Chief Information Officer (CIO)	_____
Other. Please specify: _____	_____
Do not know	_____

Section 2: Security Breach Information

8. Which of the following privacy and/or security laws is your law firm required to comply with? Please check all that apply.

Privacy and/or Security Laws	Please check all that apply
PIPEDA (The Personal Information Protection and Electronic Document Act)	_____
State Data Breach Notification Laws	_____
European Union Directive on Data Protection	_____
GLBA (Gramm-Leach-Bliley Act)	_____
HIPAA (Health Insurance Portability and Accountability Act)	_____
FACTA (Fair and Accurate Credit Transactions Act)	_____
FCRA (Fair Credit Reporting Act)	_____
USA P.A.T.R.I.O.T. Act	_____
APEC Privacy Principals (Asia Pacific Economic Cooperation)	_____
Australia's Federal Privacy Act	_____
Japan's Law Concerning the Protection of Personal Information	_____
Other. Please specify: _____	_____
Do not know	_____

11. Please indicate your level of agreement with the following statements:

Statement	Strongly Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Strongly Agree
Over the past few years, the Internet has greatly increased the number of security breaches experienced.	_____	_____	_____	_____	_____
In the coming years, the Internet will greatly increase the risk of IT security breaches.	_____	_____	_____	_____	_____

Section 3: Information Security Policies

12. Does your law firm have written information technology (IT) security policies?
Please check only one response.

Information Security Policies and Procedures	Please check only one answer
Yes	_____
No	_____
Do not know	_____

If **no** or **do not know**, please skip to question 25.

13. Were your law firm written IT security policies created due to a security incident/breach? Please check only one response.

Information Security Policies and Procedures	Please check only one answer
Yes	_____
No	_____
Do not know	_____

14. How long has your law firm been actively using a documented IT security policy?
Please check only one response.

Actively Using Information Security Policies	Please check only one answer
Days	_____
Weeks	_____
Months	_____
Years	_____
Do not know	_____

15. Approximately how often is the IT security policy updated? Please check only one answer.

IT Security Policies Updated	Please check only one answer
Never	_____
More than every 2 years	_____
Every 2 years	_____
Every year	_____
Every 6 months	_____
Less than every 6 months	_____
Do not know	_____

16. Does your law firm audit and enforce the documented IT security policy? Please check only one answer.

Audit and Enforce IT Policy	Please check only one answer
Yes	_____
No	_____
Do not know	_____

17. Approximately how often is the IT security policy audited by an independent third party? Please check only one answer.

IT Security Policies Audited	Please check only one answer
Never	_____
More than every 2 years	_____
Every 2 years	_____
Every year	_____
Every 6 months	_____
Less than every 6 months	_____
Do not know	_____

18. How is the IT security policy disseminated to law firm employees/lawyers or other members of the firm? Please check all that apply.

IT Security Policies Disseminated	Please check all that apply
Law firm Intranet	_____
Staff handbook	_____
Other. Please specify:	_____

19. Using the table below, please indicate the security issues covered in your IT security policy and/or through separate procedures or standards. If you do not explicitly cover an issue through your policy or a separate stand-alone standard, please choose not applicable (N/A).

Factors	Not At All Important	Not Very Important	Somewhat Important	Very Important	Extremely Important	Not Applicable
Effective marketing of security to all law firm employees/lawyers or other members of the firm	—	—	—	—	—	—
Distribution of guidance on IT security policy to all law firm employees/lawyers or other members of the firm	—	—	—	—	—	—
Providing appropriate training and education to all employees/lawyers or other members of the firm	—	—	—	—	—	—
Comprehensive measurement system for evaluating performance in security management	—	—	—	—	—	—
Provision of feedback system for suggesting policy improvements	—	—	—	—	—	—

21. How **successful** do you believe your law firm has been in **adopting each of these factors** on a scale of 1-5 with 1 being the least important and 5 being most important:

Factors	Not At All Successful	Not Very Successful	Somewhat Successful	Very Successful	Extremely Successful	Not Applicable
Ensuring security policy reflects business objectives	—	—	—	—	—	—
An approach to implementing security that is consistent with the law firm culture	—	—	—	—	—	—
Visible commitment from management	—	—	—	—	—	—
A good understanding of security risks	—	—	—	—	—	—
A good understanding of security requirements	—	—	—	—	—	—

Factors	Not At All Successful	Not Very Successful	Somewhat Successful	Very Successful	Extremely Successful	Not Applicable
Effective marketing of security to all law firm employees/lawyers or other members of the firm	_____	_____	_____	_____	_____	_____
Distribution of guidance on IT security policy to all law firm employees/lawyers or other members of the firm	_____	_____	_____	_____	_____	_____
Providing appropriate training and education to all employees/lawyers or other members of the firm	_____	_____	_____	_____	_____	_____
Comprehensive measurement system for evaluating performance in security management	_____	_____	_____	_____	_____	_____
Provision of feedback system for suggesting policy improvements	_____	_____	_____	_____	_____	_____

22. Are IT security policy documents approved by management? Please check only one answer.

Information Security Policies and Procedures	Please check only one answer
Yes	_____
No	_____
Do not know	_____

23. Are IT security policy documents published? Please check only one answer.

Information Security Policies and Procedures	Please check only one answer
Yes	_____
No	_____
Do not know	_____

24. Are approved IT security policy documents communicated to all law firm employees/lawyers or other members of the firm and relevant third party service providers? Please check only one answer.

Information Security Policies and Procedures	Please check only one answer
Yes – all of them are communicated to law firm employees/lawyers or other members of the firm and relevant third party service providers	<input type="checkbox"/>
Yes – but not communicated to relevant third party service providers	<input type="checkbox"/>
Yes – but only communicated to law firm employees/lawyers or other members of the firm	<input type="checkbox"/>
Yes – but only certain ones are communicated	<input type="checkbox"/>
No – none of them	<input type="checkbox"/>
Do not know	<input type="checkbox"/>

25. Are law firm computers shut down for inactivity after a defined period? Please check only one answer.

Information Security	Please check only one answer
Yes	<input type="checkbox"/>
No	<input type="checkbox"/>
Do not know	<input type="checkbox"/>

26. When under a time deadline to finish an assignment, how likely would it be for people in your law firm to:

Statement	Not At All Likely	Not Very Likely	Somewhat Likely	Very Likely	Extremely Likely
Scan a file for viruses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Install security software updates	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Install a digital certificate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Install an ActiveX control from an unknown source	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

27. Please indicate your level of agreement with the following statements:

Statement	Strongly Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Strongly Agree
The need for information security policies in law firms is greater today than it was <u>one</u> year ago.	_____	_____	_____	_____	_____
The amount of attorney-client work product communication over electronic networks is greater today than it was <u>one</u> year ago.	_____	_____	_____	_____	_____
The need for information security policies in law firms is greater today than it was <u>three</u> years ago.	_____	_____	_____	_____	_____
The amount of attorney-client work product communication over electronic networks is greater today than it was <u>three</u> years ago.	_____	_____	_____	_____	_____
The need for information security policies in law firms is greater today than it was <u>five</u> years ago.	_____	_____	_____	_____	_____
The amount of attorney-client work product communication over electronic networks is greater today than it was <u>five</u> years ago.	_____	_____	_____	_____	_____

29. Which of the following statements is true for your law firm? Please check all that apply.

Statement	Please check all that apply
There is an individual designated as being responsible for information security in my law firm.	_____
There is a separate department in my law firm responsible for information security.	_____
Information security falls upon everyone in the information technology department in my law firm.	_____
No individual is designated as being responsible for information security in my law firm.	_____

Section 4: Demographic Questions

These last few questions are to help me get to know you, the respondent, better. All of these responses are optional. Like all of the questions in this questionnaire, your answers were held in strict confidence. No answers were paired with an individual and only a cumulative set of results will be presented in the dissertation.

30. What is the highest level of education you have completed:

Education	Please check the appropriate answer
High School Graduate	_____
Paralegal Certificate	_____
Bachelor Degree	_____
Master Degree	_____
Juris Doctorate	_____
Ph.D.	_____
Other: _____	_____
Prefer not to answer	_____

31. Please state your gender:

Gender	Please check the appropriate answer
Female	_____
Male	_____

32. Please state your age:

Age	Please check the appropriate answer
18-25	<input type="checkbox"/>
26-35	<input type="checkbox"/>
36-45	<input type="checkbox"/>
46-55	<input type="checkbox"/>
56-65	<input type="checkbox"/>
65+	<input type="checkbox"/>
Prefer not to answer	<input type="checkbox"/>

33. Which title best describes your job level:

Title	Please check only one answer
Associate	<input type="checkbox"/>
Partner	<input type="checkbox"/>
Chief Information Officer/Director	<input type="checkbox"/>
Chief Security Officer/Information Security Officer	<input type="checkbox"/>
Privacy/Compliance Officer	<input type="checkbox"/>
Law Firm Administrator	<input type="checkbox"/>
Chief Executive Officer	<input type="checkbox"/>
Project Manager	<input type="checkbox"/>
Legal Technology Manager	<input type="checkbox"/>
Paralegal/Legal Assistant	<input type="checkbox"/>
Legal Secretary	<input type="checkbox"/>
Technician	<input type="checkbox"/>
Database Programmer	<input type="checkbox"/>
Database Coder	<input type="checkbox"/>
Network Administrator	<input type="checkbox"/>
Other: _____	<input type="checkbox"/>

34. Would you be willing to be contacted to answer follow-up questions via an e-mail message linking you to a second follow-up Zoomerang survey, if necessary?

* Please note that your e-mail address will only be used to send you the link to the additional survey. Any and all additional information obtained would be held in strict confidence and your name would not be used in the reporting of information.

Agree to Follow-Up Questions	Please check only one answer
Yes	<input type="checkbox"/>
If yes, please provide your e-mail address:	

No	<input type="checkbox"/>

Thank you for participating in this study! Please be advised that all responses were held in strict confidence. Your name will not be linked to your responses and your name will not be used in the reporting of information in publications or conference presentations. Only cumulative results were analyzed and placed into my dissertation. None of the completed questionnaires were reviewed by anyone other than me.

35. Is there anything additional that you would like to share with the researcher? Please provide your comments in the space provided.

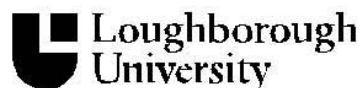
Comments:

Thank you!

Appendix F

Doherty & Fulford Original Survey Instrument

The Business School, Loughborough, LE11 3TU
Telephone: 01509 222435 Fax: 01509 269332
E-mail: H.Fulford@lboro.ac.uk



<p style="text-align: center;">IT Security</p> <p style="text-align: center;">Learning the Lessons from Practice</p>
--

**ALL RESPONSES WILL BE TREATED
IN THE
STRICTEST CONFIDENCE**

Would you like a copy of the findings: yes no

If yes, please supply name and address for receipt of your copy of the findings. Alternatively, if you would prefer your responses to remain completely anonymous, you can email Dr. Heather Fulford [h.fulford@lboro.ac.uk], to request a copy.

Name:
Address:

Please return this questionnaire in the pre-paid envelope supplied.

Section A: background information

1. Which of the following best describes the sector in which your organization primarily operates?

- | | | | | | |
|-----------------|--------------------------|----------------------|--------------------------|--------------------|--------------------------|
| Agriculture | <input type="checkbox"/> | Banking & finance | <input type="checkbox"/> | Business services | <input type="checkbox"/> |
| Construction | <input type="checkbox"/> | Education | <input type="checkbox"/> | Energy supply | <input type="checkbox"/> |
| Health | <input type="checkbox"/> | Leisure | <input type="checkbox"/> | Manufacturing | <input type="checkbox"/> |
| Public services | <input type="checkbox"/> | Transport | <input type="checkbox"/> | Wholesale & retail | <input type="checkbox"/> |
| Other | <input type="checkbox"/> | Please specify _____ | | | |

2. Which of the following best describes the geographical spread of your organisation?

- | | | | |
|--|--------------------------|--|--------------------------|
| Single site | <input type="checkbox"/> | Multiple sites, within the UK | <input type="checkbox"/> |
| Multiple sites: UK & continental Europe | <input type="checkbox"/> | Multiple sites, many continents | <input type="checkbox"/> |

3. Approximately how many people are employed in your organization?

- | | | | | | | | |
|---------------|--------------------------|-----------|--------------------------|------------|--------------------------|------------|--------------------------|
| Less than 500 | <input type="checkbox"/> | 500-1000 | <input type="checkbox"/> | 1001-1500 | <input type="checkbox"/> | 1501-2000 | <input type="checkbox"/> |
| 2001-3000 | <input type="checkbox"/> | 3001-5000 | <input type="checkbox"/> | 5001-10000 | <input type="checkbox"/> | Over 10000 | <input type="checkbox"/> |

Section B: security threats to your organization

4. Please record in the table below the **approximate number of IT security breaches** that your organization has experienced in the past two years, and **indicate the severity of the worst breach** of each type, using the scale provided.

Threats	Approximate no. of occurrences in last two years				Severity of worst incident				
					Fairly Insignificant			Highly Significant	
	0	1-5	6-10	> 10	1	2	3	4	5
Computer virus	0	1-5	6-10	> 10	1	2	3	4	5
Hacking incident (external)	0	1-5	6-10	> 10	1	2	3	4	5
Unauthorised access to / use of data (internal)	0	1-5	6-10	> 10	1	2	3	4	5
Theft of hardware / software	0	1-5	6-10	> 10	1	2	3	4	5
Computer-based fraud	0	1-5	6-10	> 10	1	2	3	4	5
Human error	0	1-5	6-10	> 10	1	2	3	4	5
Natural disaster	0	1-5	6-10	> 10	1	2	3	4	5
Damage by disgruntled employee	0	1-5	6-10	> 10	1	2	3	4	5

Section C: The Internet and the future of IT security

5. Please use the grid overleaf to indicate the strength to which you agree / disagree with each of the following two statements:

<i>Statement</i>	<i>Strongly disagree</i>			<i>Strongly agree</i>	
	1	2	3	4	5
Over the past few years, the Internet has greatly increased the number of security breaches experienced.	1	2	3	4	5
In the coming years, the Internet will greatly increase the risk of IT security breaches.	1	2	3	4	5

Section D: IT security policy

6. Does your organization have a documented IT security policy? Yes No

If no, please return your questionnaire in the envelope supplied. If yes, please answer the questions in the remaining sections of the questionnaire.

7. How long has your organisation been actively using a documented IT security policy? ____ years

8. Approximately how often is the policy updated?

Less than every 2 years Every 2 years Every year
 Every 6 months More than every 6 months

9. How is the policy disseminated to employees? Company intranet
 Staff handbook Other Please specify _____

10. Using the table below, please indicate the security issues covered in your IT security policy and/or through separate procedures or standards. If you do not explicitly cover an issue through your policy or a separate stand-alone standard, please leave blank.

IT security issue	Policy document ONLY	Stand-alone procedure or standard ONLY	Policy document AND supplementary procedure or standard
<i>Disclosure of information</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>System Access control</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Internet access</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Viruses, worms & trojans</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Software development</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Contingency planning</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Encryption</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Mobile computing</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Personal usage of IS</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Physical security</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Violations and breaches</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Section E: The Success of your IT security policy

11. Using the table below, please indicate the **importance** of each of the following factors and the extent to which your organization is **successful** in adopting them.

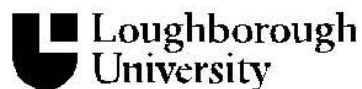
Factors	How important do you believe the following factors to be for the successful implementation of IT security in your organization?					How successful do you believe your organization has been in adopting each of these factors ?				
	<i>Not Important</i>		<i>Very Important</i>			<i>Not successful</i>		<i>Very successful</i>		
	1	2	3	4	5	1	2	3	4	5
Ensuring security policy reflects business objectives	1	2	3	4	5	1	2	3	4	5
An approach to implementing security that is consistent with the organizational culture	1	2	3	4	5	1	2	3	4	5
Visible commitment from management	1	2	3	4	5	1	2	3	4	5
A good understanding of security risks	1	2	3	4	5	1	2	3	4	5
A good understanding of security requirements	1	2	3	4	5	1	2	3	4	5
Effective marketing of security to all employees	1	2	3	4	5	1	2	3	4	5
Distribution of guidance on IT security policy to all employees	1	2	3	4	5	1	2	3	4	5
Providing appropriate employee training and education	1	2	3	4	5	1	2	3	4	5
Comprehensive measurement system for evaluating performance in security management	1	2	3	4	5	1	2	3	4	5
Provision of feedback system for suggesting policy improvements	1	2	3	4	5	1	2	3	4	5

Please use this space if you wish to make any comments with respect to the formulation, application or effectiveness of IT security policy within your organisation

Appendix G

Revised Doherty & Fulford Original Survey Instrument

The Business School, Loughborough, LE11 3TU
 Telephone: 01509 222435 Fax: 01509 269332
 E-mail: H.Fulford@lboro.ac.uk



IT Security

Learning the Lessons from Practice

**ALL RESPONSES WILL BE TREATED
 IN THE
 STRICTEST CONFIDENCE**

~~The following questions have been removed since my dissertation survey already has these particular questions covered.~~

~~Would you like a copy of the findings: yes no~~

~~If yes, please supply name and address for receipt of your copy of the findings. Alternatively, if you would prefer your responses to remain completely anonymous, you can email Dr. Heather Fulford (h.fulford@lboro.ac.uk), to request a copy.~~

Name:
Address:

~~Please return this questionnaire in the pre-paid envelope supplied.~~

Section A: background information

1. Which of the following best describes the sector in which your organization primarily operates?

Agriculture Banking & finance Business services
 Construction Education Energy supply
 Health Leisure Manufacturing
 Public services Transport Wholesale & retail
 Other Please specify _____

2. Which of the following best describes the geographical spread of your organisation?

Single site Multiple sites, within the UK
 Multiple sites: UK & continental Europe Multiple sites, many continents

3. Approximately how many people are employed in your organization?

Less than 500 500-1000 1001-1500 1501-2000
 2001-3000 3001-5000 5001-10000 Over 10000

Section B: security threats to your organization law firm

4. Please record in the table below the **approximate number of IT security breaches** that your **organization law firm** has experienced in the past two years, and **indicate the severity of the worst breach** of each type, using the scale provided. **Zoomerang will not allow me to double up the answers like displayed below.** Thus, I will ask the "Severity of the worst breach" question underneath the "occurrence in last two years" question. They will both be on the same page online at Zoomerang.com.

Threats	Approximate no. of occurrences in last two years				Severity of worst incident				
					Fairly Insignificant		Highly Significant		
Computer virus	0	1-5	6-10	> 10	1	2	3	4	5
Hacking incident (external)	0	1-5	6-10	> 10	1	2	3	4	5
Unauthorized access to / use of data (internal)	0	1-5	6-10	> 10	1	2	3	4	5
Theft of hardware / software	0	1-5	6-10	> 10	1	2	3	4	5
Computer-based fraud	0	1-5	6-10	> 10	1	2	3	4	5
Human error	0	1-5	6-10	> 10	1	2	3	4	5
Natural disaster	0	1-5	6-10	> 10	1	2	3	4	5
Damage by disgruntled employee	0	1-5	6-10	> 10	1	2	3	4	5

Section C: The Internet and the future of IT security

5. Please use the grid overleaf to indicate the strength to which you agree / disagree with each of the following two statements:

<i>Statement</i>	<i>Strongly disagree</i>			<i>Strongly agree</i>	
	1	2	3	4	5
Over the past few years, the Internet has greatly increased the number of security breaches experienced.	1	2	3	4	5
In the coming years, the Internet will greatly increase the risk of IT security breaches.	1	2	3	4	5

Section D: IT security policy

6. Does your **organization law firm** have a documented IT security policy? Yes No

If no, please return your questionnaire in the envelope supplied skip to question _____. If yes, please answer the questions in the remaining sections of the questionnaire.

7. How long has your **organization law firm** been actively using a documented IT security policy?
_____ years

8. Approximately how often is the policy updated?

Less More than every 2 years Every 2 years Every year
Every 6 months More than every 6 months

9. How is the policy disseminated to **law firm** employees/attorneys? Company intranet
Staff handbook Other Please specify _____

10. Using the table below, please indicate the security issues covered in your IT security policy and/or through separate procedures or standards. If you do not explicitly cover an issue through your policy or a separate stand-alone standard, please leave blank.

IT security issue	Policy document ONLY	Stand-alone procedure or standard ONLY	Policy document AND supplementary procedure or standard
<i>Disclosure of information</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>System Access control</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Internet access</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Viruses, worms & trojans</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Software development</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Contingency planning</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Encryption</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Mobile computing</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

IT security issue	Policy document ONLY	Stand-alone procedure or standard ONLY	Policy document AND supplementary procedure or standard
Personal usage of IS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Physical security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Violations and breaches	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Section E: The Success of your IT security policy

11. Using the table below, please indicate the **importance** of each of the following factors and the extent to which your **organization law firm** is **successful** in adopting them. Zoomerang will not allow me to double up the answers like displayed below. Thus, I will ask the “the successful implementation of IT security” question underneath the “adopting each of these factors” question. They will both be on the same page online at Zoomerang.com.

Factors	How important do you believe the following factors to be for the successful implementation of IT security in your organization law firm ?					How successful do you believe your organization law firm has been in adopting each of these factors ?				
	Not Important		Very Important			Not successful		Very successful		
Ensuring security policy reflects business objectives	1	2	3	4	5	1	2	3	4	5
An approach to implementing security that is consistent with the organization law firm culture	1	2	3	4	5	1	2	3	4	5
Visible commitment from management	1	2	3	4	5	1	2	3	4	5
A good understanding of security risks	1	2	3	4	5	1	2	3	4	5
A good understanding of security requirements	1	2	3	4	5	1	2	3	4	5
Effective marketing of security to all law firm employees/ attorneys	1	2	3	4	5	1	2	3	4	5
Distribution of guidance on IT security policy to all law firm employees/ attorneys	1	2	3	4	5	1	2	3	4	5
Providing appropriate employee training and education	1	2	3	4	5	1	2	3	4	5
Comprehensive measurement system for evaluating performance in security management	1	2	3	4	5	1	2	3	4	5
Provision of feedback system for suggesting policy improvements	1	2	3	4	5	1	2	3	4	5

Please use this space if you wish to make any comments with respect to the formulation, application or effectiveness of IT security policy within your **organization law firm**.

Reference List

- Alagna, T., Chen, E., Cirino, M., Elliott, C., Elron, R., Foster, S. W., et al. (2005). *Larstan's: The Black Book on Corporate Security*. North Potomac, MD: Larstan Publishing, Inc.
- Arora, A., Nandkumar, A., & Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers*, 8, 350-362.
- Baker, W. H. & Wallace, L. (2007). Is information security under control? Investigating quality in information security management. *IEEE Security & Privacy*, 5(1), 36-44.
- Bartlett, D. & Smith, L. (2008). Managing the data loss crisis. *Risk Management*, 55(6), 34-37.
- Basta, A. & Halton, W. (2008). *Computer Security and Penetration Testing*, Boston, MA: Thomson Course Technology.
- Batista, C. (2006). Better safe than sorry: Assessing internal security on your firm's network. *International Legal Technology Association (ILTA) Whitepaper*, *ILTAnet.org, Cracking the Code on Security*, 3-5.
- Belsis, P. & Kokolakis, S. (2005). Information systems security from a knowledge management perspective. *Information Management & Computer Security*, 13(2/3), 189-202.
- Beaver, K. (2007). *Hacking for Dummies, 2nd Edition*, Indianapolis, IN: Wiley Publishing, Inc.
- Berg, G. G., Freeman, M. S. & Schneider, K. N. (2008). Analyzing the TJ Maxx data security fiasco: Lessons for auditors. *The CPA Journal*, 78(8), 34-37.
- Bisel, L. D. (2007). The role of SSL in cybersecurity. *IT Professional*, 9(2), 22-25.
- Bowen, P., Hash, J., & Wilson, M. (2006). *Information security handbook: A guide for managers*. *NIST Special Publication 800-100*. Retrieved November 20, 2009, from <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>.
- California Senate Bill 1386 – SB 1386. (2002, March 20). *California Senate bill no. 1386: Chapter 915*. *California Senate*. Retrieved November 20, 2009, from http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.

- Cannoy, S., Palvia, P.C., & Schilhavy, R. (2006). A research framework for information systems security. *Journal of Information Privacy & Security*, 2(2), 3-29.
- Carnegie Mellon University. (2007). Welcome to US-CERT vulnerability notes database. *Cert.org*. Retrieved November 20, 2009, from <http://cve.mitre.org/about/faqs.html#b3>.
- Cassini, J. A., Medlin, B.D., & Romaniello, A. (2008). Law and regulations dealing with information security and privacy: An investigative study. *International Journal of Information Security and Privacy*, 2(2), 70-82.
- Chandler, J. A. (2007). Negligence liability for breaches of data security. *Banking & Finance Law Review*, 23, 223-272.
- Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy & Security*, 1(3), 18-41.
- Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology, Learning, and Performance Journal*, 24(1), 1-14.
- Centers for Medicare & Medicaid Services – CMS. (2003). HIPAA administrative simplification – security: Final rule. *Federal Register*, 68(34), 8334-8381.
- Cocheo, S. (2006). Read this before you take multi-factor plunge. *American Bankers Association, ABA Banking Journal*, 98(5), 54-55.
- Comerford, J. D. (2006). Competent computing: A lawyer's ethical duty to safeguard confidentiality. *The Georgetown Journal of Legal Ethics*, 19, 629-642.
- Conger, S. (2009). Personal information privacy: A multi-party endeavor. *Journal of Electronic Commerce in Organizations*, 7(1), 71-82.
- Congress of the United States of America. (2009). American Recovery and Reinvestment Act of 2009, *WhiteHouse.gov*. Retrieved October 10, 2009, from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf.
- Creswell, J. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches Third Edition*. Thousand Oaks, CA: Sage Publications, Inc.
- Creswell, J. W. & Clark, V. L. P. (2007). *Designing and Conducting Mixed Methods Research*. Thousand Oaks, CA: Sage Publications, Inc.

- Curtin, C. M. & Ayres, L. T. (2009). Using science to combat data loss: Analyzing breaches by type and industry. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), 569-601.
- D'arcy, J. & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics: Supplement*, 89, 59-71.
- Da Veiga & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, 24(4), 361-371.
- Desouza, K. C. (2008). The neglected dimension in strategic sourcing: security. *Strategic Outsourcing: an International Journal*, 1(3), 288-292.
- Doherty, N. F. & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal*, 18(4), 21-39.
- Doherty, N. F. & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25, 55-63.
- Evans, J. R. & Mathur, A. (2005). The value of online surveys. *Internet Research*, 15(2), 195-219.
- Farn, K-J., Lin, S-K., & Lo, C-C. (2008). A study on e-Taiwan information system security classification and implementation. *Computer Standards & Interface*, 30(1), 1-7.
- Federal Deposit Insurance Corporation – FDIC. (2004, December). Putting an end to account-hijacking identity theft study. *FDIC.gov*. Retrieved October 26, 2009, from http://192.147.69.84/consumers/consumer/idtheftstudy/identity_theft.pdf.
- Federal Deposit Insurance Corporation – FDIC. (2005, June 17). Putting an end to account-hijacking. Identity theft study supplement. *FDIC.gov*. Retrieved November 26, 2009 from <http://www.fdic.gov/consumers/consumer/idtheftstudysupp/idtheftsupp.pdf>.
- Federal Financial Institutions Examination Council – FFIEC. (2005, October 12). Authentication in an Internet banking environment. Retrieved November 20, 2009, from http://www.ffiec.gov/pdf/authentication_guidance.pdf.
- Federal Trade Commission. (2005). FACTA disposal rule goes into effect June 1. *FTC.gov*. Retrieved November 20, 2009, from <http://www.ftc.gov/opa/2005/06/disposal.shtm>.

- Federal Trade Commission. (2007). Identity theft Red Flags and address discrepancies under the Fair and Accurate Credit Transactions Act of 2003 final rule. *FTC.gov*. Retrieved November 20, 2009, from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2007_register&docid=07-5453-filed.pdf.
- Field, A. (2009). *Discovering Statistics Using SPSS (3rd Ed.)*. Thousand Oaks, CA: Sage Publications, Inc.
- Foley, M. F. (2008). The FTC's Web site privacy and security rules for every business. *Computer and Internet Lawyer*, 25(12), 15-21.
- Fordham, D. R. (2008). How strong are your passwords? *Strategic Finance*, 89(11), 42-47.
- FTC Business Alert. (2005, June). Disposing of consumer report information? New rule tells how. *FTC.gov*. Retrieved November 20, 2009, from <http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt152.pdf>.
- Fulford, H. & Doherty, N. (2003). The application of information security policies in large UK-based organizations: An exploratory investigation. *Information Management & Computer Security*, 11(3), 106-114.
- Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, 25(1), 27-35.
- Garrison, C. P. (2008). An evaluation of passwords. *The CPA Journal*, 78(5), 70-71.
- Gibney, C. & Corham, T. (2008). *ILTA's 2008 technology survey*. Retrieved January 1, 2009, from http://www.iltanet.org/communications/pub_detail.aspx?nvID=000000011205&h4ID=000001315505.
- Goldberg, J. (2008). The evolution of the law firm risk. *Risk Management*, 55(8), 48-53.
- Gorga, E. & Halberstam, M. (2007). Knowledge inputs, legal institutions and firm structure: Towards a knowledge-based theory of the firm. *Northwestern University Law Review*, 101(3), 1123-1206.
- Gramm-Leach-Bliley – GLBA. (1999). Gramm-Leach-Bliley Act: The financial modernization act. *FTC.gov*. Retrieved November 20, 2009, from <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>.
- Greenberg, P. (2008, December). Right to know. *State Legislatures*, 26-29.

- Greenberg, P. (2009). State security breach notification laws. *NCSL.org*. Retrieved November 20, 2009, from <http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx>.
- Greene, S. S., (2006). *Security Policies and Procedures: Principles and Practices*, Upper Saddle River, NJ: Pearson Education, Inc.
- Gunasekara, G. (2007). The 'final' privacy frontier? Regulating trans-border data flows. *International Journal of Law and Information Technology*, 15(3), 362-393.
- Gupta, A. & Hammond, R. (2005). Information systems security issues and decisions for small business: An empirical examination. *Information Management & Computer Security*, 13(4), 297-310.
- Hadfield, G. K. (2008). Legal barriers to innovation: The growing economic cost of professional control over corporate legal matters. *Stanford Law Review*, 60(6), 1689-1732.
- Hagen, J. M., Albrechtsen, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4), 377-397.
- Harrison, W. (2006). Passwords and passion. *IEEE Software*, 23(4), 5-7.
- Heikkila, F. M. (2006). Information security assessment of law firm networks. *Journal of Business and Behavioral Sciences*, 14(1), 123-134.
- Heikkila, F. M. (2007). Encryption: Security considerations for portable media devices. *IEEE Security & Privacy*, 5(4), 22-27.
- Heitzenrater, J. A. (2008). Data breach notification legislation: Recent developments. *I/S: A Journal of Law and Policy for the Information Society*, 4(3) 661-680.
- Hildebrand, M. J., & Savare, M. (2008). Privacy principles for accountants. *The CPA Journal*, 78(5), 54-59.
- Hiltgen, A., Kramp, T., & Weigold, T. (2006). Secure Internet banking authentication. *IEEE Security & Privacy*, 4(1), 21-29.
- Holloway, M. & Fensholt, E. (2009). HITECH: HIPAA gets a facelift. *Benefits Law Journal*, 22(3), 85-89.
- Hook, B. (2009). Reducing risk. *SC Magazine*, 20(5), 26-28.

- Hong, K-S., Chi, Y-P, Chao, L. R., & Tang, J-H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, 14(2), 104-115.
- Humphreys, E. (2007). *Implementing the ISO/IEC 27001:Information Security Management System Standard*, Boston, MA: Artech House.
- Im, G. P. & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *Database for Advances in Information Systems*, 36(4), 68-79.
- International Standards Organization (ISO) and International Electrotechnical Commission (IEC) 27001 Joint Technical Committee. (2005). *Information security management system requirements*. (ISO/IEC 27001:2005). London: British Standards Institution.
- International Standards Organization (ISO) and International Electrotechnical Commission (IEC) 27002 Joint Technical Committee. (2005). *Information technology - Code of practice for information security management*. (ISO/IEC 27002:2005). London: British Standards Institution.
- ITRC – Identity Theft Resource Center. (2008a). ITRC 2008 data breach list. *IDTheftCenter.org*, Retrieved November 20, 2009, from http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_2008_final_1_1.pdf.
- ITRC – Identity Theft Resource Center. (2008b). 2008 data breach stats. *IDTheftCenter.org*, Retrieved November 20, 2009, from http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_Report_2008_final_1.pdf.
- ITRC – Identity Theft Resource Center. (2009). 2008 data breach total soars. *IDTheftCenter.org*, Retrieved November 20, 2009, from http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Total_Soar_printer.shtml.
- Johnson, V. R. (2008). Data security and tort liability. *Journal of Internet Law*, 11(7), 22-31.
- Johnston, A. C. and Warkentin, M. (2008). Information privacy compliance in the healthcare industry. *Information Management & Computer Security*, 16(1), 5-19.
- Jones, M. E. (2008). Data breaches: Recent developments in the public and private sectors. *I/S: A Journal of Law and Policy for the Information Society*, 3(3) 555-580.

- Kahn, S. & Sheshadri, V. (2008). Medical record privacy and security in a digital environment. *IT Pro*, 10(2), 46-52.
- Kamal, M. (2008). The psychology of IT security in business. *Journal of American Academy of Business, Cambridge*, 13(1), 145-150.
- Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Security Management*, 22(2), 7-19.
- Kemp, M. (2005). Beyond trust: Security policies and defence-in-depth. *Network Security*, 2005(8), 14-16.
- Kent, K. & Souppaya, M. (2006). Guide to computer security log management. *NIST Special Publication 800-92*. Retrieved November 20, 2009, from <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>.
- Kim, E. B. (2005). Information security awareness status of full time employees. *The Business Review, Cambridge*, 3(2), 219-226.
- Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38(2), 143-154.
- Kugele, N. & Placer, J. (2007, July). Navigating some uncertain waters in Michigan's new security breach notification law. *Privacy & Data Security Law Journal*, 710-737.
- LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for Internet safety. *Communications of the ACM*, 51(3), 71- 76.
- Lefferts, J. (2009). Patrick administration's final data security regulations filed and take effect March 1, 2010: State received notice of more than 1 million instances of exposure in two years, *Mass.gov*. Retrieved November 20, 2009, from http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=20091104_idtheft&csid=Eoca.
- Li, J. & Shaw, M. J. (2008). Electronic medical records, HIPAA, and patient privacy. *International Journal of Information Security and Privacy*, 2(3), 45-54.
- Lin, P. P. (2006). System security threats and controls. *The CPA Journal*, 76(7), 58-66.
- Massachusetts General Laws. (2008). Security breaches: Regulations to safeguard personal information of Commonwealth residents, *Mass.gov*. Retrieved November 20, 2009, from <http://www.mass.gov/legis/laws/mgl/93h-2.htm>.

- Massachusetts Office of Consumer Affairs and Business Regulation. (2009). 201 CMR 17.00: Standards for the protection of personal information of residents of the Commonwealth, *Mass.gov*. Retrieved November 20, 2009, from <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>.
- McMillion, R. (2006). Case closed. *ABA Journal*, 92, 66, 68.
- Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the vulnerability of U.S. hospitals to social engineering attacks: How many of your employees would share their password? *International Journal of Information Security & Privacy*, 2(3), 71-83.
- Metzler, M. (2007). Promoting security policy longevity. *Computer Security Journal*, XXIII, (2/3), 82-94.
- Miller, M. Z. (2007). Why Europe is safe from ChoicePoint: Preventing commercialized identity theft through strong data protection and privacy laws. *The George Washington International Law Review*, 39(2), 395-421.
- Moscaritolo, A. (2009, July 30). Red Flags delay. *SC Magazine*. Retrieved October 11, 2009, from <http://www.scmagazineus.com/Red-Flags-delay/article/140888/>.
- Myler, E. & Broadbent, G. (2006). ISO 17799: Standard for security. *The Information Management Journal*, 40(6), 43-52.
- Nahra, K. J. (2008). HIPAA security enforcement is here. *IEEE Security & Privacy*, 6(6), 70-72.
- Nelson, S. D., Isom, D. K., & Simek, J. W. (2006). *Information Security for Lawyers and Law Firms*. Chicago, IL: ABA Publishing.
- Nickell, C. G. & Denyer, C. (2007). An introduction to SAS 70 audits. *Benefits Law Journal*, 20(1), 58-68.
- NSU Institutional Review Board. (2008). Institutional Review Board for research with human subjects (IRB) continuation/renewal/renewal of research protocol. *Nova Southeastern University*. Retrieved November 20, 2009, from <http://www.nova.edu/irb/process.html>.
- Open Security Foundation. (2008). Data loss database 2008 yearly report. *DataLossDB.org*. Retrieved November 20, 2009, from http://datalosdb.org/yearly_reports/dataloss-2008.pdf.

- Otto, P. N., Antón, A. I., & Baumer, D. L. (2007). The ChoicePoint dilemma: How data brokers should handle the privacy of personal information. *IEEE Security & Privacy*, 5(5), 15-23.
- Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods (3rd Ed.)*. Thousand Oaks, CA: Sage Publications, Inc.
- PCI Security Standards Council LLC. (2008). Payment Card Industry Data Security Standard (DSS) v 1.2. Retrieved November 20, 2009, from https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.
- Pfleeger, S. L. & Rue, R. (2008). Cybersecurity economic issues: Clearing the path to good practice. *IEEE Software*, 25(1), 35-42.
- PIPEDA (The Personal Information Protection and Electronic Documents Act). (1998). Privacy Act. Retrieved November 20, 2009, from http://www.priv.gc.ca/legislation/02_06_01_e.cfm.
- Podgers, J. (2008). A new mission. *ABA Journal*, 94(12), 60.
- Podgers, J. (2009). Wells: FTC delay on 'Red Flag Rule' aids ABA effort. *ABA Journal*, 95(9), 64-65.
- Post, G. V. & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computer & Security*, 26(3), 229-237.
- Power, R. (2002). 2002 CSI/FBI computer crime and security survey. *Computer Security Issues & Trends*, VII(1), 1-24. Retrieved November 20, 2009, from <http://diogenesllc.com/2002cybercrimesurvey.pdf>.
- Privacy Rights Clearinghouse. (2008). A chronology of data breaches. *PrivacyRights.org*. Retrieved November 20, 2009, from <http://www.privacyrights.org/ar/ChronDataBreaches.htm#1>.
- Punter, T., Ciolkowski, M., Freimut, B. & John, I. (2003). Conducting on-line surveys in software engineering. *International Symposium of Empirical Software Engineering*, 80-88.
- Radcliff, D. (2008). Slurping the USB port. *SC Magazine*, 19(9), 30-31.
- Raether, R. I. Jr. (2008). Data security and ethical hacking: Points to consider for eliminating avoidable exposure. *Business Law Today*, 18(1), 55-58.
- Ramim, M. & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology*, 8(4), 24-34.

- Reinstein, A. & Seward, J. (2008). Client-CPA-attorney privilege and information technology risk. *The CPA Journal*, 78(11), 66-71.
- Rey, J. (2008). Are you “red flag” ready? *American Bankers Association – ABA Banking Journal*, 100(7), 47-50.
- Richardson, R. (2006). Headstrong passwords. *Computer Security Journal*, XXII(2), 7 – 10.
- Richardson, R. (2009). 2008 CSI computer crime and security survey. *GOCSI.com*. Retrieved November 20, 2009, from <http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf>.
- Ries, D. (2007). Information security for attorneys: An ethical obligation. *Pennsylvania Bar Association Quarterly*, 78(1), 1-14.
- Robinson, T. (2005). Data security in the age of compliance. *netWorker*, 9(3), 24-30.
- Romanosky, S., Telang, R., & Acquisti, A. (2008). Do data breach disclosure laws reduce identity theft? *Seventh Workshop on the Economics of Information Security*, Hanover, NH, June 25-28, 1-20.
- Ross, R. (2007). Managing enterprise security risk with NIST standards. *Computer*, 40(8), 88-91.
- Roster, C. A., Rogers, R. D., Hozier, G. C., Baker, K. G., & Albaum, G. (2007). Management of marketing research projects: Does delivery method matter anymore in survey research? *Journal of Marketing Theory and Practice*, 15(2), 127-144.
- Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal*, 42(6), 32-34, 36-38.
- Salmela, H. (2008). Analysing business losses caused by information systems risk: A business process analysis approach. *Journal of Information Technology*, 23(3), 185-202.
- Sarbanes-Oxley Act of 2002. (2002, July 30). *H.R. 3763, Public Law 107, 116 Stat. 745-810*. Retrieved November 20, 2009, from <http://www.soxlaw.com/>.
- Schreft, S. L. (2007). Risks of identity theft: Can the market protect the payment system?. *Economic Review – Federal Reserve Bank of Kansas City*, 92(4), 5-40.
- Schwartz, P. M. & Janger, E. J. (2007). Notification of data security breaches. *Michigan Law Review*, 105(5), 913-984.

- Sekaran, U. (2003). *Research Methods for Business: A Skill Building Approach*. New York, NY: John Wiley & Sons.
- Silverman, D. L. (2007). Data security breaches: The state of notification laws. *Intellectual Property & Technology Law Journal*, 19(7), 5-12.
- Sinkovics, R. R., Penz, E., & Ghauri, P. N. (2008). Enhancing the trustworthiness of qualitative research in international business. *Management International Review*, 48(6), 689-713.
- Siponen, M. & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems*, 7(7), 445-472.
- Siponen, M. T. & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *The Database for Advances in Information Systems*, 38(1), 60-80.
- Stream, G. & Fletcher, J. (2008). Demystifying computer networks for small practices. *Family Practice Management*, 15(1), 25-28.
- Sveen, F. O., Sarriegi, J. M., Rich, E., & Gonzalez, J. J. (2007). Towards viable information security reporting systems. *Information Management & Computer Security*, 15(5), 408-419.
- Swartz, N. (2008). Record data breaches in 2008. *Information Management Journal*, 42(6), 20.
- Swire, P. P. & Bermann, S. (2007). *Information Privacy: Official Reference for the Certified Information Privacy Professional (CIPP)*, York, ME: International Association of Privacy Professionals.
- Taylor, E., & Murthy, U. (2009). Knowledge sharing among accounting academics in an electronic network of practice. *Accounting Horizons*, 23(2), 151-179.
- Thomson, K-L. & von Solms, R. (2006). Towards an information security competence maturity model. *Computer Fraud & Security*, 2006(5), 11-15.
- U. S. Department of Commerce. (2000). Safe Harbor certification. *Export.gov*. Retrieved November 20, 2009, from <http://www.export.gov/safeharbor/>.
- Verdon, D. (2006). Security policies and the software developer. *IEEE Security & Privacy*, 4(4), 42-49.
- Walton, R. B. (2009, October 30). Order granting Plaintiff's motion for summary judgment. Retrieved November 20, 2009, from http://www.abanet.org/media/docs/ABA_v._FTC_Amended_Order.pdf.

- Weaver, R. (2007). *Guide to Network Defense and Countermeasures Second Edition*. Boston, MA: Thomson Course Technology.
- Wernick, A. S. (2009, July/August). Red Flags Rule: Will you be compliant or complacent? *Ohio Lawyer*, 14-17.
- West, R. (2008). The psychology of security. *Communications of the ACM*, 51(4), 34-40.
- Whitman, M. E. & Mattord, H. J. (2008). *Management of Information Security Second Edition*. Boston, MA: Thomson Course Technology.
- Wiant, T. L. (2005). Information security policy's impact on reporting security incidents. *Computers & Society*, 24, 448-459.
- Worthen, B. (2008, October 16). New data privacy laws set for firms. *The Wall Street Journal*. Retrieved November 20, 2009, from <http://online.wsj.com/article/SB122411532152538495.html>.
- Wugmeister, M., Retzer, K. & Rich, C. (2007). Global solution for cross-border data transfers: Making the case for corporate privacy rules, *Georgetown Journal of International Law*, 38(3), 449-498.