INFORMATION SECURITY IN THE AGE OF CLOUD COMPUTING

A Dissertation
presented in partial fulfillment of requirements
for the degree of Doctor of Philosophy
in the Patterson School of Accountancy
The University of Mississippi

by

J. ERIC SIMS, CPA, CMA

April 2012

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

ABSTRACT

Information security has been a particularly hot topic since the enhanced internal control requirements of Sarbanes-Oxley (SOX) were introduced in 2002. At about this same time, cloud computing started its explosive growth. Outsourcing of mission-critical functions has always been a gamble for managers, but the advantages of cloud computing are too tempting to ignore. However, the move to cloud computing could prove very costly for a business if the implementation were to fail. When making the decision to outsource critical functions, managers look to accountants to provide assurance that their data and transactions will be secure and that emergency procedures will be in-place and work as designed, to protect the business from any potential losses due to unforeseen events.

Statement on Auditing Standards (SAS) 70 has provided guidance to auditors of third-party service organizations since 1992, but was replaced in April 2010 by Statement on Standards for Attestation Engagements (SSAE) 16. And yet, data breaches continue to occur, costing billions of dollars annually.

This research used data from the Privacy Rights Clearinghouse (PRC) database and, through frequency analysis, Chi-square and cluster analysis techniques, found statistically significant differences in the frequency of breaches experienced by various types of consumer organizations based on breach and organization type. This result will be useful to auditors. The research also conducted a survey of 67,749 IT manager/directors. The responses to this survey were to be analyzed using binary logistic regressions and Chi-square tests. Unfortunately, due to

severe limitations in the response rate and further complicated by the number of incomplete responses, no inferences can be drawn regarding factors relevant to decision-makers when contemplating the movement of critical business functions into the cloud environment.

LIST OF ABBREVIATIONS

AICPA	American Institute of Certified Public Accountant
CICA	Canadian Institute of Chartered Accountants
CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology
EDP	Electronic Data Processing
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IAASB	International Auditing and Assurance Standards Board
IC	Internal Controls
IRB	Institutional Review Board
ISACA	Information System Audit and Control Association
ISAE	International Standards for Assurance Engagements
IT	Information Technology
NIST	National Institute of Standards and Technology
PRC	Privacy Rights Clearinghouse
PaaS	Platform as a Service
Saas	Software as a Service
SAP	Statement on Auditing Procedure
SAS	Statement on Auditing Standards

SOC	Service Organization Control
SOX	Sarbanes-Oxley Act of 2002
SSAE	Statement on Standards for Attestation Engagements

ACKNOWLEDGEMENTS

I would first like to acknowledge my dissertation committee: Dr. Dale Flesher (Chair), Dr. Brian Reithel, Dr. Karl Wang and Dr. Mitch Wenger. I thank each of you for your time, intellectual contributions, and your unwavering support throughout my time in this graduate program. I have truly enjoyed working with you and appreciate you for making this dissertation such a rewarding experience. I would like to add a very special thank you to Dr. Dale Flesher – he is the reason I came to the University of Mississippi. He is my mentor, idol and friend.

TABLE OF CONTENTS

ABSTRACT ii

LIST OF ABBREVIATIONS iii

ACKNOWLEDGEMENTS iv

LIST OF TABLES ix

LIST OF FIGURES xii

CHAPTER I – INTRODUCTION 1

Historical Overview 4

Information Assurance 4

Early Guidance 4

SAS70 5

Sarbanes-Oxley (SOX) 5

Cloud Computing 6

Recent Events 7

SSAE16 7

ISAE3402 8

AICPA Service Organization Control (SOC) Reports 9

Motivation 9
Research Purpose and Questions 10
Research Design and Methodology 11
Sample 12
Importance of the Research 14
Theory 15
Results 18
Contributions of the Research 19
Limitations of the Research 20
Organization of the Dissertation 21
CHAPTER II – LITERATURE REVIEW 22
History of Service Provider Assurance 22
Early Guidance 22
Statement on Auditing Standards (SAS) No. 70 23
Trust Services 27
SysTrust 28
Statement on Standards for Attestation Engagements (SSAE) No. 16 30
AICPA Service Organization Control (SOC) Reports 31
History of Cloud Computing 34
Essential Characteristics of Cloud Computing 34

Cloud Service Models 36
Cloud Deployment Models 38
Pros and Cons 40
Growth 43
Recent Breach History 44
Cost of Breaches 51
Cloud-specific Breach Issues 52
CHAPTER III – METHODOLOGY 57
Research Design 58
Sample 59
Variables 59
Hypotheses 64
Tests 67
CHAPTER IV – RESULTS 72
Research Question One 72
Research Question Two 85
Research Question Three 102
CHAPTER V – CONCLUSIONS 110
Contributions of the Research 113
Future Research 115

BIBLIOGRAPHY 117

APPENDICES 125

Appendix 1 – Survey Instrument 126

Appendix 2 – IRB Approval 130

Appendix 3 – Monthly Data 132

Appendix 4 – Annual Data 134

Appendix 5 – Breach Type by Org Type Data 136

Appendix 6 – Non-Significant Trends by Breach Type 138

Appendix 7 – Breach and Organization Frequency Data 141

Appendix 8 – Hypothesis 4 Supporting Tables 143

Appendix 9 – Tables for Hypothesis 6 Testing 148

Appendix 10 – Tables for Hypothesis 7 Testing 150

VITA 152

LIST OF TABLES

Table 1 - PRC Descriptive Data 45

Table 2 – Significance Test of Breach Frequency Trend 74

Table 3 – Significance Test of "DISC" Trend 76

Table 4 - Significance Test of "HACK" Trend 77

Table 5- Significance Test of "CARD" Trend 78

Table 6 - Significance Test of "INSD" Trend 79

Table 7 - Significance Test of "PHYS" Trend 80

Table 8 - Significance Test of "PORT" Trend 81

Table 9 – Significance Test of Total Breach Frequency by Breach Type 83

Table 10 – Significance Test of Total Breach Frequency by Organization Type 85

Table 11 - Association between Breach Type and Org Type 87

Table 12 - Significance Test for "Other" Business Sector 89

Table 13 - Significance Test for Financial Business Sector 90

Table 14 - Significance Test for Retail Business Sector 92

Table 15 - Significance Test for Education Sector 93

Table 16 - Significance Test for Governmental Sector 95

Table 17 - Significance Test for Medical Sector 97

Table 18 - Significance Test for Non-profit Sector 99

Table 19 - Overall Cluster Distribution 100

Table 20 - Clusters based on Breach Type 100
Table 21 - Clusters based on Organization Type 101
Table 22 - Frequency Data for Survey Questions 4a & 4b 103
Table 23 - Future Outsourcing Intent 104
Table 24 - Importance of 3rd-Party Service Provider Audits 105
Table 25 - Survey Response Frequency 106
Table 26 - Cloud Use 107
Table 27 - 3rd-party Service Provider Audited? 107
Table 28 – Reported Importance of 3rd-party Service Provider Audit Reports 108
Table 29 - Knowledge of 3rd-party Service Provider Reporting 109
Table 30 – Breaches by Type by Month 133
Table 31 - Breaches by Type by Year 135
Table 32 - Breach Type by Organization Type 137
Table 33 – Non-significant “STAT” Trend 139
Table 34 - Non-significant "UNKN" Trend 140
Table 35 - Supporting Data for Figure 9 142
Table 36 - Supporting Data for Figure 10 142
Table 37 - Supporting Data for Figure 11 144
Table 38 - Supporting Data for Figure 12 144
Table 39 - Supporting Data for Figure 13 145
Table 40 - Supporting Data for Figure 14 145
Table 41 - Supporting Data for Figure 15 146
Table 42 - Supporting Data for Figure 16 146

Table 43 - Supporting Data for Figure 17 147

Table 44 – Future Intent versus Importance Placed on Assurance Services (Hypothesis 6) 149

Table 45 – Hypothesis 6 Chi-square Result 149

Table 46 – Hypothesis 6 Binary Logistic Regression Result 149

Table 47 – Future Intent versus Assurance Knowledge Level (Hypothesis 7) 151

Table 48 – Hypothesis 7 Chi-square Result 151

Table 49 – Hypothesis 7 Binary Logistic Regression Result 151

LIST OF FIGURES

Figure 1 - Cloud Computing Environment....40
Figure 2 - Conceptual Model....63
Figure 3 – Total Breaches Trend Analysis....73
Figure 4 - "DISC" Trend....75
Figure 5 - "HACK" Trend....76
Figure 6 - "CARD" Trend....77
Figure 7 - "INSD" Trend....79
Figure 8 - "PHYS" Trend....80
Figure 9 - "PORT" Trend....81
Figure 10 – Percent of each Breach Type of Total Breach Frequency....82
Figure 11 – Percent of Total Breach Frequency by Organization Type....84
Figure 12 - Breaches for "Other" Sector Business Entities....88
Figure 13 - Breaches for Financial Sector Entities....90
Figure 14 - Breaches for Retail Sector Entities....91
Figure 15 - Breaches for Educational Sector Entities....93
Figure 16 - Breaches for Governmental Sector Entities....95
Figure 17 - Breaches for Medical Sector Entities....97
Figure 18 - Breaches for Non-profit Sector Entities....98
Figure 19 - IRB Approval....131

Figure 20 - "STAT" Trend.....139

Figure 21 - "UNKN" Trend.....140

Chapter I

INTRODUCTION

Responsibility for information assurance, and therefore the requirement for expertise in the area, has always been a part of the accountant's domain due to the critical nature of the information underlying the accuracy and reliability of the financial statements. Historically, the focus has always been limited to financial information and the underlying data. However, with the increase in use of the internet to not only transmit data, but to also process and store it, users have begun to expect much more from the assurance offered by auditors of service provider organizations. Accountants have been involved with computers since they were first introduced and have continued to expand their level of responsibility as computerized systems have grown more powerful and their use more widespread. However, since the passage of the Sarbanes-Oxley act in 2002, which required enhanced internal control reporting requirements by management and expression of an opinion by external auditors on an internal control report, the expectations for the level of assurance have increased dramatically. This "raising of the bar" is evidenced by the enhanced requirements placed on an auditor as written directly into the legislation.

As a concept, Cloud Computing has been around since the early 1960s, but the majority of its transition from concept to practice has occurred within the past decade. This coincides with the increased level of accountants' responsibility for providing assurance on information above and beyond the financial arena, which was partially driven by users' persistence in relying on audit reports to represent assurance beyond that which was intended. Cloud computing involves moving business-critical data and processing to location(s) external to the company's own computer hardware. These external storage locations and processing capacities are typically obtained from third-party "service providers". Outsourcing of mission-critical functions will always involve risks, and cloud computing is certainly no exception. But the efficiencies that can be obtained through the use of cloud computing technologies are being confirmed as factual versus speculative and should not be disregarded – to do so in today's super-competitive global environment may lead to missed opportunities. Still, managers must remember that the move to cloud computing is fraught with complications that could prove disastrous for a business if even a single implementation were to fail. A major consideration for all managers is the security of the data once it is in the cloud. There is still a lot of doubt in this area, due to the ever-present and growing incidence of data breaches. In his *New York Times* small-business guide on moving to the cloud, David Freedman quotes sources as saying "A lot of my older clients don't want any of their data in the cloud" and "They're very nervous about it." Another source, Mike Leatherwood of a barbecue restaurant chain states that he "is an enthusiastic user of Google Apps, but he agrees that confidential data should be kept out of the cloud. 'We keep financial and H.R. data on our servers here,' he said." Mr. Freedman advises, "The bottom line: If you do not like the idea of trusting anyone but yourself to keep your data safe, the cloud may take you

out of your comfort zone." (Freedman, 2011). Consequently, when making the decision to outsource critical functions, business managers naturally look to accountants to provide assurance that their data and transactions will be secure, and that emergency procedures will be in-place and work as designed, to protect the business from any potential losses due to unforeseen events. The early guidance on providing assurance services to third-party service providers was fairly limited with regard to any focus other than financial. In order to properly analyze the impact of Information Assurance on Cloud Computing, it is appropriate to first define what is meant by each of these terms.

According to the U.S. National Information Assurance Glossary, Information Assurance refers to offering "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." (Committee on National Security Systems, 2010).

For purposes of this study, the term Cloud Computing will be limited in meaning to the description provided by the U.S. National Institute of Standards and Technology (NIST), which defines Cloud Computing as:

> A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources – for example networks, servers, storage, applications and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction (Badger, Grance, Patt-Corner, & Voas, 2011).

Cloud Computing allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports

them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud). Both the user's data and essential security services may reside in and be managed within the network cloud (Richard Kissel, 2011). All model components are described in further detail in chapter II.

Historical Overview

Information Assurance

Early Guidance

Consideration of an entity's internal control goes back to the very first Statement on Auditing Procedure (SAP) issued in 1939. However, guidance that specifically addressed the effects of Electronic Data Processing (EDP) on the auditor's study and evaluation of internal control was not introduced until 1974, with the release of Statement on Auditing Standards (SAS) No. 3. Even with this shift in focus, this pronouncement was not specific to service organizations, but applied to EDP functions in general. The first guidance issued to specifically address the impact of the internal control system of a third-party service organization was SAS No. 44, issued in December of 1982. This was soon followed by SAS No. 48 in July of 1984, titled "The Effects of Computer Processing on the Audit of Financial Statements. Over the next several years, outsourcing of many business functions became commonplace. Consequently, the regulatory authorities acknowledged the need to provide guidance that would specifically

address the evaluation of the internal control structure of third-party service providers. This was achieved by the issuance of SAS No. 70, titled “Service Organizations”.

SAS70

Since its creation in 1992 by the AICPA, Statement on Auditing Standards (SAS) 70 has provided guidance to auditors of third-party service organizations when conducting audits to provide such assurance on the internal control structure of the service organization. SAS70 is designed to enable an independent auditor to evaluate and issue an opinion on a service organization's controls. It does not specify a pre-determined set of control objectives or control activities that service organizations must achieve – i.e., it is not a "checklist" audit. It does, however, enable an independent auditor ("service auditor") to issue an opinion on a service organization's controls through a Service Auditor's Report. There are two types of Service Auditor's Reports: Type I and Type II. A Type I report only describes the service organization's description of controls at a specific point in time (e.g. December 31, 2010). Alternatively, a Type II report also includes detailed testing of the service organization's controls over a minimum six-month period (e.g. July 1, 2010 to December 31, 2010). So the complete service auditor's report contains the auditor's opinion, a description of the controls placed in operation, and if the report is a Type II, a description of the auditor's tests of operating effectiveness. The audit report can then be shared with the service organization's customers ("user organizations") and their respective auditors ("user auditors"), eliminating the need for audits of controls of the service organization by the auditors of each client organization.

Sarbanes-Oxley (SOX)

On July 30, 2002, Congress passed the “Sarbanes-Oxley Act of 2002”, which had a major impact on the responsibility for and reporting on internal control within a business. Section 404

specifically requires management to prepare a report asserting that they have examined their "internal control over financial reporting" structure and have implemented the appropriate controls to assure the accuracy of the financial information. The section further stipulates that the external auditor of the organization's financial statements must also perform an examination of the internal controls (IC) of the company and express an opinion on management's IC statement. According to an article written by Christopher L. Schellman, co-founder of SAS70 Solutions, "Many public companies, as part of their respective efforts to achieve compliance under Section 404, discovered that certain financial reporting controls that they relied upon were actually maintained by outsourced third-party service providers." (Schellman 2005) That is to say, to be considered compliant a company must verify that its service provider's controls, in addition to its own, are effective (Bell III, 2010).

Cloud Computing

Cloud computing is not actually as new a concept as many people would believe, since the general idea behind it dates back to the 1960s. However, the idea saw little movement toward practical implementation for the next several decades. In the early 1990s, an idea called "grid computing" became popular. This was a concept named for its intent to make computer power as easy to access as an electric power grid, and it is grid computing that is credited for leading to the current cloud computing paradigm.

The origin of the term "cloud computing" is uncertain, but many attribute it to the diagrams of clouds used to represent the internet in journals and textbooks. The concept was developed by telecommunications companies who made a radical shift in their processing methodology. By optimizing resource utilization through load balancing, they could get their

work done more efficiently and inexpensively. One of the earliest major players in cloud computing was Salesforce.com, which in 1999 introduced the concept of delivering enterprise applications via a website. Amazon quickly followed, launching Amazon Web Service in 2002. When Google Docs joined the movement in 2006, cloud computing really began its rapid increase in popularity. Also in 2006 Amazon introduced "Elastic Compute cloud" (EC2), as a commercial web service that allowed small companies and individuals to rent computers on which to run their own applications. The year 2007 saw the implementation of an industry-wide collaboration between Google, IBM and a number of universities across the United States. This was followed in 2008 by Eucalyptus, which was the first open source platform for deploying private clouds, and OpenNebula, the first open source software for deploying private and hybrid clouds. Microsoft finally got in the game in 2009, with the launch of Windows Azure in November of that year. Since 2009, Oracle, Dell, Fujitsu, Teradata, HP, and many other well-known technology companies have introduced their own cloud-based service divisions.

Recent Events

SSAE16

Following the introduction of SAS70 in 1992, there was little change in the guidance for service provider auditors until April of 2010, when it was replaced by Statement on Standards for Attestation Engagements (SSAE) 16. This new guideline was designed to more closely align U.S. policy with the International Standard on Assurance Engagements (ISAE) 3402, which was released in December of 2009.

Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, was issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in April 2010, and effectively replaces SAS70 as the standard for reporting on service organizations. It has a mandatory effective date of June 15, 2011. SSAE16 was drafted and issued with the intention and purpose of updating the US service organization reporting standard so that it mirrors and complies with the new international service organization reporting standard. The new standard is an attest standard and not an audit standard. Consequently, it will require management to provide the service auditor a written assertion about the fair presentation of the description of the service organization's system, the suitability of the design of the controls and, in the case of a Type II report, the operational effectiveness of the control. This is a substantial departure from the guidance provided under SAS70.

ISAE3402

International Standards for Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization, was issued in December 2009 by the International Auditing and Assurance Standards Board (IAASB). Like SSAE16, it has a mandatory effective date of June 15, 2011. ISAE3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting (ISAE3402.com, 2011).

AICPA Service Organization Control (SOC) Reports

SSAE16 and ISAE3402 were drafted in part to prevent SAS70 audits from being misused to imply assurance on non-financial aspects (compliance and operations) of the internal control structure of a service organization. To help CPAs examine the controls and to help management understand the related risks, the AICPA has established three Service Organization Control (SOC) reports (SOC 1, SOC 2 and SOC 3).

SOC 1 engagements are performed in accordance with SSAE16. They focus solely on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. SOC 2 and SOC 3 engagements address controls at the service organization that relate to operations and compliance, such as data security, availability, processing integrity and online privacy. These are the only report types that provide assurance specific to a third-party provider's data and processing security, yet they are neither mandatory nor are they official regulation.

Motivation

In spite of the best efforts of auditors and regulators, however, there still seem to be some inadequacies in the system designed to assure data security. This is evidenced by the fact that breaches of purportedly secure and safe data systems continue to occur. Many researchers believe that the logical first step in resolving such an issue is to clearly define the current state of affairs. Wallace, et al. opine "Establishing baseline knowledge of the current state of organizational controls is essential to achieving the ultimate goal of developing and testing a model linking IT controls to SOX compliance success." (Wallace, Lin, & Cefaratti, 2011)

Consequently, this research will attempt to identify areas where data breaches are most prevalent in an attempt to identify sections within the information assurance services arena that could be strengthened. This will aid in the battle against potential future data breaches, because specific identification of areas of vulnerability will lead to development of improved and/or enhanced assurance procedures that may decrease the likelihood of data breaches, thereby enhancing the value of information assurance services. Also, inefficiencies in the current system can be eliminated by providing auditors with specific guidance on where best to focus their energies.

Research Purpose and Questions

It should be noted that a major assumption underlying this research is that the proportion of reported breaches to actual breaches does not change. There is no evidence found that would suggest that the ratio of reported to unreported breaches would change, and it is a necessary assumption to this research when examining trends.

Purpose: To empirically establish that experienced breach frequency varies significantly between various pairings of breach type and organization type. This information may greatly assist auditors in the risk assessment portion of their engagement planning, as the engagement activities can be focused on addressing those breach events more likely to occur, based on organization type. An additional objective is to empirically determine if SAS70/SSAE16/SOC audit services affect the decisions of Chief Information Officers (CIOs) regarding their consideration of whether or not to employ cloud/datacenter-hosted solutions and examine their

level of awareness regarding the different assurance levels offered by these various third-party service provider audit reports.

The objective of this research is to answer the following questions:

1. Are there any significant anomalies in reported breach data that could be used to benefit auditors?
2. If type of organization is significantly associated with type of breach, which organization types are most vulnerable to which types of breaches?
3. Do any of the following influence CIOs when making outsourcing (cloud) decisions?

   Prior breach experience
   Level of importance placed on audit certification
   Level of personal knowledge of assurance levels

Research Design and Methodology

The research design will be two-fold. The first portion of the study will utilize available data on the frequency and type of data breaches experienced by various types of organizations. This data will be analyzed using standard statistical analysis techniques, such as frequency analysis, cluster analysis and Chi-squared statistics to address research questions one and two. The second part of the study will utilize data obtained from a survey that was administered via email to 67,749 IT directors throughout the U.S. This data will also be analyzed using multiple statistical analysis techniques, including binomial logistic regression and Chi-squared analysis, to address research question three.

Sample

The data for the first part of this study were obtained from the Privacy Rights Clearinghouse (PRC) database[1]. Privacy Rights Clearinghouse purports to be *a nationally recognized consumer education and advocacy nonprofit dedicated to protecting the privacy of American consumers.* The organization's employees compile information on reported data breaches from a multitude of sources, including the Open Security Foundation list-serve, Databreaches.net, PHI Privacy and NAID. Personal Health Information Privacy (PHI Privacy) is a database that compiles only medical data breaches. Many of these are obtained from the US Department of Health and Human Services' medical data breach list. National Association for Information Destruction, Inc (NAID) provides monthly newsletters that include a number of data breaches largely due to improper document destruction. Data for the PRC database has been collected since April of 2005, but actually includes data for breaches starting in January of 2005. The database is updated every two days. The breaches posted into this database are limited to those occurring within the United States and specifically do not include incidents in other countries. By PRCs own admission, it is not a complete listing of breaches. The list is a useful indication of the types of breaches that occur, the categories of entities that experience breaches, and the size of such breaches. But the list is not a comprehensive listing. Reported incidents affecting more than nine individuals from an identifiable entity are included. Breaches affecting nine or fewer individuals are included if there is a compelling reason to alert consumers. Most of the information is derived from the Open Security Foundation listserv, which is in turn derived from verifiable media stories, government web sites/pages, or blog posts with information pertinent to the breach in question. If a breached entity has failed to notify its customers or a government agency of a breach, then it is unlikely that the breach will be reported anywhere

[1] Used with the permission of the Privacy Rights Clearinghouse, www.privacyrights.org.

(PRC-FAQ, 2012). But many breaches are reported as a result of state requirements that individuals be notified in the event that their personal data has been breached. The catalyst for reporting data breaches to the affected individuals has been the California law that requires notice of security breaches, implemented in July of 2003. Since then, more than 40 states have passed laws requiring that individuals be notified of security breaches. For the period under investigation, a total of 2,847 breaches were reported. This data will be predominantly analyzed on a monthly basis.

The data for the second part of the study comes from a survey that was emailed to 67,749 IT directors at various educational, for-profit, governmental, medical, and non-profit organizations located throughout the United States. The survey participants were selected based on their inclusion in a database of IT directors employed in these various organization types and ostensibly employed at the appropriate level to answer the survey questions. This database was purchased from SpecialDatabases.com, and has the following characteristics:

Primary Email - 100% Fill Ratio

Contact Title - 100% Fill Ratio

First Name - 100% Fill Ratio

Last Name - 100% Fill Ratio

Company Name - 100% Fill Ratio

Address - 100% Fill Ratio

City - 100% Fill Ratio

State - 100% Fill Ratio

Zip Code - 100% Fill Ratio

Phone - 100% Fill Ratio

Fax Number

SIC Code - 100% Fill Ratio

NAICS Code - Industry - 100% Filling Ratio

Website Address - 100% Filling Ratio

Statistical analysis of the survey responses was used to address research question three. Specific procedures conducted are described in greater detail below.

Importance of the Research

In the current ultra-competitive, global business environment, the question for most managers is *when* to make the move to the cloud, not *if*. Growth of the cloud computing industry, as measured by revenues, has been substantial over the past decade and all projections are that the level of growth will not only continue, but will accelerate. In order to garner a share of this potential market, third-party service providers need to overcome the main concerns of consumers. In recent years, security has consistently been reported as the #1 concern, as reported in numerous surveys and frequently proclaimed in the popular media outlets. Consequently, for those providers that can effectively negate this concern, growth seems all but certain. This research is important because it will provide information that auditors of third-party cloud service providers can use during their audits to bolster the security aspect of their work as it pertains to data breaches. This will aid the auditing profession, because as more consumers gain a comfort level and place greater reliance on the work of auditors, more work will become available through the growth of the cloud computing industry. This should evolve as a result of hesitant consumers overcoming their fears and choosing to embrace the technology.

Theory

The concept under investigation here is that of outsourcing of computerized functions and the attempts to manage the inherent risks associated with that activity. There are numerous theories that support the outsourcing decision. In one of the more comprehensive recent studies, Gottschalk & Solli-Sæther (2006) examine critical issues at various stages of maturity in the outsourcing relationship. They conclude that at the beginning of an outsourcing engagement, a Cost Stage occurs, which is grounded in Transaction Cost Economics (TCE) and agency theory. After several years of having outsourcing, the focus of the outsourcer shifts into the Resource Stage, where resource based view (RBV) and core competences are the most important explanatory theories. At the end, the stage of Partnership may occur, when relational view, social exchange, and the stakeholders theories become more explanatory (Gottschalk & Solli-Sæther, 2006).

Transaction Cost Economics (TCE) has been the most used theory of outsourcing (Perunovic & Pedersen, 2007). A transaction cost is a cost incurred in making an economic exchange. Many studies have concluded that due to economies of scale, service vendors have a clear cost advantage. Consequently, outsourcing of computer storage and data processing functions (cloud computing) has become an almost required component for many businesses to remain competitive in today's global markets. Some authors suggest that it is cost prohibitive to prevent breaches at all levels, but many companies are willing to accept the risk anyway because the realized benefits outweigh the potential cost. The current research's goal of reducing the effective cost of cloud computing, by enhancing audit efficiencies, would lend further support to organizations opting to outsource based on this theory.

Agency theory is a consideration in the outsourcing decision due to the nature of the arrangement – i.e., transferring of responsibility from the company to its agent (cloud service provider). Concerns generated by the agency problem (moral hazards and adverse selection) can be resolved by monitoring and bonding (Clegg, Hardy, & Nord, 1996). What makes this part of the outsourcing arrangement particularly difficult is that transfer of the responsibility for processing and storage of data does not transfer the fiduciary responsibility of the consumer company to those from which the data emanated.

The resource-based view (RBV) of the firm theory holds that firms possess resources, a subset of which enable them to achieve competitive advantage, and a subset of those that lead to superior long-term performance. The resource-based view in outsourcing builds from a proposition that an organization that lacks valuable, rare, inimitable and organized resources and capabilities, shall seek for an external provider in order to overcome that weakness (Wernerfelt, 1984).

The concept of core competences is built on the resource-based theory. The concept originally supported keeping all of the business critical processes "in-house". It was based on the idea that core competencies were the "collective learning" of the organization and that knowledge base was to be coveted. Interestingly, it is now applied to outsourcing because the outsource vendor's competences are assumed to be incorporated into the consumer organization competencies. It is now considered one of the most important factors that influence success of an outsourcing arrangement (Feeny, Lacity, & Willcocks, 2005). Assuming the current research is able to identify audit efficiencies for third-party service providers, the level of reliance that consumers feel they can place on the security offered by third-party service providers will

increase. This will, in turn, allow more consumer organizations to rely on this reasoning to justify their outsourcing decision.

The relational view theory is closely related and tied to the RBV theory and to the concept of core competencies. It is based on the premise that a firm's critical resources may span firm boundaries and may be embedded in interfirm routines and processes (Dyer & Singh, 1998). Here again, this theory supports the decision to outsource critical functions as a means of gaining competitive advantage, when an organization does not have the necessary expertise in-house.

Social exchange theory is defined as "limited to actions that are contingent on rewarding reactions from others. Implied is a two-sided, mutually contingent, and mutually rewarding process involving "transactions" or simply "exchange" (Emerson, 1976). It addresses the utility of establishing mutually beneficial relationships, as cloud service providers and consumers are motivated to do. In order to maintain the mutually beneficial nature of the relationship, service providers must ensure that they provide what the customer wants and needs – in this case, data security in the cloud.

The stakeholder theory is a basis of outsourcing logic that is applicable to every business entity. This theory argues that every person or other entity that participates in the operation of an organization does so in order to obtain benefits (Perunovic & Pedersen, 2007). Cloud providers only participate in the relationship in order to sell their services. Likewise, cloud consumers will only participate in the relationship if the perceived level of benefit (data security) matches their requirement.

The need to demonstrate adequate control of data and processing security is critical to all third-party "cloud" services providers – failure to do so will likely result in lost revenues. Unless

a third-party provider can confirm assurance of the level of security required, consumer organizations will not be able to justify establishing a relationship based on any of these theories.

Results

The results of the first research question indicate that anomalies do exist that may benefit auditors of third-party service providers. A significant trend in breach patterns by month over time was identified. It was also determined that significant trends do exist in the frequency of breaches by both breach type and by organization type. The analysis of research question two further refined the relationship between breach types and organization types and provides the opportunity to make recommendations for specific focus areas based on organization type under audit. This will prove quite valuable to auditors. Research question three sought to identify factors that influence IT directors regarding prior breach experience and their willingness to continue to outsource key business functions. There were some observations noted in the frequency analysis of the survey data that may prove interesting and/or useful for future research. Unfortunately, due to a severely limited response rate, statistical verification of suspected relationships was not possible. It also sought to determine if the level of certification of auditor services as relates to third-party service providers is or is not important to the IT managers of consumer entities. Again, data limitations precluded this testing. Finally, the question remains unanswered as to whether managers claiming an understanding of the differences between SAS70/SSAE16/SOC and SOC type 2 & 3 reports are more or less likely to rely on those higher-level assurances when making their outsourcing decisions.

Contributions of the Research

Assuming existing vulnerabilities to data breaches as identified by this project are addressed through future audit guidance, this research will benefit: 1) CPA firms that provide Information Assurance services to third-party service provider organizations, as they will have better guidance and can plan and conduct their audit services more efficiently and effectively, 2) third-party service provider companies (those that consume SAS70/SSAE16/SOC audit services), as they may reduce their breach frequency, which will enhance their image and their audits may be more efficient and therefore less costly, 3) CPA firms that audit cloud consumer organizations, because they can place more reliance in the work of the service organization auditor, and finally, 4) the cloud services consumer organizations themselves, as they may experience lower audit fees through efficiencies recognized in 3) above. All of this may also promote enhanced trust in cloud systems and therefore, growth of the industry. The ultimate contribution of this research will be that it will provide additional tools to regulators and auditors, which they can use in the fight against the ever-growing problems associated with data breaches – i.e., identity theft, financial fraud, etc. These events are extremely expensive; not only to individuals, but to society in general, as the economic losses experienced by businesses are ultimately passed through to consumers. Governmental agencies will also benefit from enhanced audit procedures. So too will taxpayers, since the costs of losses experienced by governmental organizations are borne by society either through reductions in services or the additional tax dollars necessary to compensate for the economic losses due to breaches. Finally, educational institutions also stand to gain considerably from this research, as they too are frequent victims of data breaches and suffer the associated economic penalties.

Limitations of the Research

All empirical studies suffer from certain limitations and this one is no exception. Using data from past periods is a good method of generalizing what has occurred and identifying trends. It does not, however, predict the future. The best that research can hope for is to draw reasonable conclusions as to what the future may hold. Another limitation is in the data itself. The data from the Privacy Rights Clearinghouse has limitations imposed by the manner in which it is accumulated. For example, there are likely to be breaches that go unreported and are therefore not included in the current analyses. It is possible that some of these may even be significant. This study is also limited to breaches reported in the U. S. and may not be generalizable to populations taken from other geographic regions or combinations thereof. The second portion of the research relied on a survey instrument administered via email. Survey instruments have inherent limitations due to their very nature. One of the most notable of these is non-response bias. Non-response bias refers to the mistake one expects to make in estimating a population characteristic based on a sample of survey data in which, due to non-response, certain types of survey respondents are under-represented (Berg, 2005). Another survey limitation is that the questions must be general enough to be appropriate for all respondents and may therefore not elicit a response that could prove useful to the research. Finally, the survey portion of this particular research is severely limited by a dismal response rate. Statistical analysis of the data proved meaningless and no inferences can be made based on the survey results.

Organization of the Dissertation

The remainder of this dissertation is organized as follows: Chapter II presents a review of the previous literature outlining the history of Information Assurance as it pertains to third-party service providers. It also includes a history of Cloud Computing (outsourcing), an examination of the pertinent data breach information, and a review of the literature that specifically addresses Information Assurance issues in cloud computing. Chapter III summarizes the methodology to be employed to test the hypotheses, including a list of significant variables utilized, and a description of the tests to be conducted. Chapter IV explains the results of the analyses performed, and Chapter V outlines the conclusions of the research, its limitations, and suggestions for future research.

Chapter II

LITERATURE REVIEW

History of Service Provider Assurance

Early Guidance

Consideration of an entity's internal control goes back to the very first Statement on Auditing Procedure (SAP) issued in 1939. The level of importance placed on the issue was raised with the release of SAP No. 29 in 1958, which further delineated the scope of the auditor's review of internal control. As the use of computerized processing became more prevalent, updated pronouncements had to be released to address the issues raised. The first official pronouncement to specifically address the effects of Electronic Data Processing (EDP) on the auditor's study and evaluation of internal control was SAS No. 3, which was released in December of 1974. This pronouncement was not specific to service organizations, but applicable to all EDP functions that impacted the financial statements of the organization under audit.

The first guidance issued to specifically address the impact of the internal control system of a third-party service organization was Statement on Auditing Standards (SAS) No. 44, issued in December of 1982. It provided guidance on preparation of "Special-Purpose Reports on Internal Accounting Control at Service Organizations". This was soon followed by SAS No. 48 in July of 1984, titled "The Effects of Computer Processing on the Audit of Financial Statements. Over the next several years, outsourcing of many business functions, including some that had a substantial impact on the financial statements, became commonplace. Consequently, the regulatory authorities acknowledged the need to provide guidance that would specifically address the evaluation of the internal control structure of third-party service providers. This was achieved by the issuance of SAS No. 70, titled "Service Organizations", which was the first attempt at combining the requirements of internal control of third-party service providers, computerized processing and financial reporting into one regulation.

Statement on Auditing Standards (SAS) No. 70

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is a widely recognized auditing standard developed in 1992 by the American Institute of Certified Public Accountants (AICPA). SAS70 is generally applicable when an independent auditor ("user auditor") is planning the financial statement audit of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that impact a user organization's system of internal controls could be application service providers, bank trust departments, claims processing centers, data centers, third-party administrators, or other data processing service bureaus. If a service organization provides transaction processing, data hosting, IT infrastructure, or other data processing services to the user organization, the user

auditor may need to gain an understanding of the controls at the service organization in order to properly plan the audit and evaluate control risk (SAS70.com, 2011).

An auditor's examination performed in accordance with SAS No. 70, commonly referred to as a "SAS70 Audit", represents that a service organization has been through an in-depth audit of its control objectives and control activities, which often include controls over information technology and related processes. The service organization is responsible for describing its control objectives and control activities that would be of interest to user organizations and the respective user auditors. In order to entice businesses to consume cloud service offerings, service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. The requirements of Section 404 of the Sarbanes-Oxley Act of 2002 makes service auditor reports even more important to the process of reporting on the effectiveness of internal control over financial reporting.

SAS70 was created to help auditors specifically address the internal controls of a service organization as they pertain to the financial statements. Unfortunately, it is written in such a manner as to allow substantial interpretation because it does not specify any pre-determined of control objectives or control activities that must be met in order for a service organization to "pass". This flexibility has been abused in the past to imply more assurance on the IC of the service organization than what might actually exist. While SAS70 does provide an auditor the opportunity to issue an opinion on a service organization's controls through a Service Auditor's Report, the reports are limited to only two types: Type I and Type II. A Type I report only describes the service organization's description of controls at a specific point in time (e.g. December 31, 2010). Alternatively, a Type II report also includes detailed testing of the service organization's controls over a minimum six-month period (e.g. July 1, 2010 to December 31,

2010). So the complete service auditor's report contains the auditor's opinion, a description of the controls placed in operation, and if the report is a Type II, a description of the auditor's tests of operating effectiveness. The audit report can then be shared with the service organization's customers ("user organizations") and their respective auditors ("user auditors"), eliminating the need for audits of controls of the service organization by the auditors of each client organization. Regardless of which report is issued, it still only addresses those controls that might have a material effect on the financial statements.

In other words, in a Type I report, the service auditor will express an opinion and report on the subject matter provided by the management of the service organization as to (1) whether the service organization's description of its system fairly presents the service organization's system that was designed and implemented as of a specific date; and (2) whether the controls related to the control objectives stated in management's description of the service organization's system were suitably designed to achieve those control objectives – also as of a specified date.

In a Type II report, the service auditor will express an opinion and report on the subject matter provided by the management of the service organization as to (1) whether the service organization's description of its system fairly presents the service organization's system that was designed and implemented throughout the specified period; (2) whether the controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period to achieve those control objectives; and (3) whether the controls related to the control objectives stated in management's description of the service organization's system operated effectively throughout the specified period to achieve those control objectives (Reehl, 2011).

One of the major limitations to SAS70 is that it was specifically targeted toward providing assurance for financial reporting purposes. Unfortunately, as the need for other types of assurance (compliance and operational) grew, many service providers began misrepresenting the scope and level of assurance provided by their SAS70 compliance. SAS70 audits were not designed for nor are they appropriate for meeting assurance needs over many cloud offerings in the areas of infrastructure, platform, or software as a service. Recently, the topics of Business Continuity and Disaster Recovery have taken on increased significance as customer organizations attempt to understand how capable their service provider is of handling a business interruption. The increasing sophistication of computer viruses and events such as the catastrophe of September 11th, 2001, have demonstrated that organizations must have contingency plans in place to mitigate such risks. Organizations that use a third-party service organization are now heavily vested in the adequacy of their service provider's business continuity and disaster recovery abilities. Historically, service providers have included a control objective related to business continuity in their description of controls as part of the SAS70 audit. However, business continuity planning addresses how an organization mitigates future risks; it does not provide actual controls that give user auditors any assurance. Because of this ambiguity, the AICPA has provided the following:

> "A service organization's plans related to business continuity and contingency planning generally is of interest to the management of user organizations. If a service organization wishes to describe its business continuity and contingency plans, such information may be included in Section Four (4), "Other Information Provided by the Service Organization." Because plans are not controls, a service organization should not include in its description of controls (Section Two of the

report) a control objective that addresses business continuity or contingency planning." (AICPA, 2010).

If a service organization wants to further advertise the adequacy of its business continuity activities, it should employ a Trust Services attestation engagement using the Trust Services Availability principle.

Trust Services

Trust Services are defined as a set of professional assurance and advisory services based on a common framework to address the risks and opportunities of IT. These principles provide guidance when offering assurance services, advisory services, or both on information technology (IT)-enabled systems. This framework is particularly relevant when providing services with respect to security, availability, processing integrity, privacy, and confidentiality (AICPA, 2012). Trust Services Principles and Criteria are:

Security –	The system is protected against unauthorized access (both physical and logical).
Availability –	The system is available for operation and use as committed or agreed.
Processing Integrity –	System processing is complete, accurate, timely, and authorized.
Online Privacy –	Personal information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.
Confidentiality –	Information designated as confidential is protected as committed or agreed.

SysTrust

SysTrust is the AICPA's early attempt to address the limitations in the SAS70 audit framework and offer an alternative approach. SysTrust is a specific service model jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). A SysTrust engagement allows public accounting firms and practitioners to provide assurance on the reliability of a system using any of the Trust Services Principles and Criteria. It is designed to increase the comfort of management, customers, and business partners with systems that support a business or particular activity. In a SysTrust engagement, the practitioner evaluates and tests whether a specific system is reliable when measured against three essential principles: availability, security, and integrity.

At the completion of a SysTrust engagement, the practitioner renders an opinion on management's assertion (or the actual subject matter) that effective controls were maintained to provide reasonable assurance that the SysTrust principles were achieved. The practitioner can report on all four SysTrust principles or each principle separately. Because the SysTrust principles and criteria are established and available to any user, the practitioner's report does not have to be restricted to specific parties. Consequently, the resulting Trust Services report can be distributed to a much wider audience, which means it can provide additional value to the service organization. Trust Services help address issues that SAS70, SSAE16 and ISAE3402 are not designed to cover.

Another common criticism of SAS70 audits is that the service organization defines the objectives of the audit, leading some to question the validity of the audit from the onset. Scott Crawford, research director at Enterprise Management Associates (EMA) and former information security officer for the International Data Centre of the Comprehensive Nuclear-

Test-Ban Treaty Organization in Vienna, Austria phrases it as "A SAS70 audit is conducted according to objectives defined by the service organization for itself. In other words, SAS70 is not itself a framework of objectives, but rather allows the organization to choose its objectives -- which begs the question of 'audited to what?'" (Brenner, Data Protection, 2010). A better approach, at least in eyes of many critics of SAS70, is to perform service organization audits based on some pre-defined list of criteria rather than only audit those controls that management identifies. In this manner, audit services would be seen as offering substantially more value and the audit reports would become more consistent between third-party service providers. Numerous lists of control risks exist upon which to base this type of examination, such as ISO 27001/27002 (from the Greek word isos, meaning equal) and COBIT (Control OBjectives for Information and related Technology).

The ISO 27001/27002 standard has over 150 predefined controls. Auditors can use the list to identify all the controls that should apply to the situation at hand and then implement procedures to test those controls. This methodology prevents management from only providing assurance on those controls that they know are in place and operating properly. COBIT, first released in 1996 by the Information System Audit and Control Association (ISACA), is an IT governance framework that helps managers reconcile control requirements, technical issues and business risks. It enables clear policy development and good practice for IT control throughout organizations, and emphasizes regulatory compliance. CobIT has proven so popular that a new release (COBIT 5) is scheduled for release later in 2012. Sadly, the newest guidance, Statement on Standards for Attestation Engagements No. 16, does not incorporate either of these guidelines and does little to address the issue of only affirming what management asserts. Management is not likely to request assurance reports on controls that they know are weak or missing.

Statement on Standards for Attestation Engagements (SSAE) No. 16

Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, was issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in April, 2010. SSAE16 effectively replaces SAS70 as the standard for reporting on service organizations with an effective date of June 15, 2011. SSAE16 was issued with the intention of updating the US service organization reporting standard so that it mirrors and complies with the new international service organization reporting standard ISAE3402. There are many similarities between SAS70 and SSAE16. For example, the scope still focuses on controls relevant to internal controls over financial reporting, and the auditor's report will still be restrictive in nature. Some critics indicate that the new regulation will be just a rehash of the old one. In the opinion of Chris Schellman, President of SAS70 Solutions, Inc., "We may actually be entering a boom period for "SAS70 v2.0" (in the form of SSAE16 and ISAE3402). Most differences between SAS70 and the new standards will be almost indistinguishable to the average layperson" (Brenner, Data Protection, 2010). The key differences noted between SAS70 and SSAE16 are: 1) the newer regulation requires that the report contain a written assertion in the body of the report about the fair presentation of the description of the service organization's system, the suitability of the design of the controls and, for Type 2 reports, the operating effectiveness of the controls (because SSAE16 is an Attestation standard, whereas SAS70 was an Audit standard), and 2) SSAE16 prohibits the use of prior evidence.[2]

So it would appear that the new regulation has primarily focused on shifting the responsibility for the control activity back to management of the service provider organization,

[2] SAS70 allowed auditors to use evidence gathered in prior audits in support of the current examination. SSAE16 specifically disallows this practice.

rather than enhancing the audit process itself. It seems that the importance of strengthening internal controls and the tests of those controls has again been lost in the shuffle. It is also noted that this guidance still leaves unfulfilled the need to provide assurance on "other than financial" processes, specifically the data handling and storage processes. Fortunately, the AICPA has provided direction in these other areas through the issuance of Service Organization Control Reports (SOC) guidelines.

AICPA Service Organization Control (SOC) Reports

As previously noted, one of the presumed motivations behind the drafting of SSAE16 and ISAE3402 was to prevent SAS70 audits from being misused to imply assurance on non-financial aspects (compliance and operations) of the internal control structure of a service organization. But SSAE16 fell short of addressing these other areas. To remedy the SSAE16 limitations in this respect, the Assurance and Advisory Services section of the AICPA has created three Service Organization Control (SOC) reports to help fill the gap.

SOC 1 engagements are performed in accordance with SSAE16. They focus solely on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. The two types of SOC 1 reports are similar to the two SAS70 reports, the difference being that the auditor's reports now report on "management's description" of the system of internal controls and suitability to achieve the specified control objectives. Type 1 reports are still as of a specific date and type 2 reports are still for a specific period of time. Distribution of these reports is restricted to existing user entities. An example would be: An employee benefit plan uses a bank trust department to invest and service the plan's assets. When the employee benefit plan's financial statements are audited, the plan's auditor needs information

about the plan's internal control over financial reporting, including controls at the bank trust department that affect the employee benefit plan's financial statements. The plan's auditor can obtain that information from an SOC type 2 report, which provides the service auditor's opinion on whether the controls were operating effectively at the bank and describes tests of the controls performed by the service auditor to form that opinion and the results of those tests.

SOC 2 guidance is designed to assist CPAs in reporting on the effectiveness of a service organization's controls related to operations and compliance. This new guide combines the Trust Services criteria (related to security, availability, processing integrity, confidentially or privacy) with the reporting detail provided by SSAE16 to help service organizations provide their user entities with the information their auditors need. Both type 1 and type 2 reports may be issued for SOC 2 engagements. Type 1 reports provide a description of the service organization's system, with type 2 reports also including a description of the tests performed and the results of those tests. Because of the detailed description of tests performed, distribution of this report is limited to user organizations. An example of an application of this type would be: A Cloud Service Organization that offers virtualized computing environments or services for user entities wishes to assure its customers that the service organization maintains the confidentiality of its customers' information in a secure manner and that the information will be available when it is needed. A SOC 2 report addressing security, availability and confidentiality provides user entities with a description of the service organization's system and the controls that help achieve those objectives.

SOC 3 engagements are similar to SOC 2 engagements. Both use the predefined criteria in Trust Services Principles, Criteria and Illustrations and both address controls at the service organization that relate to operations and compliance. The big difference is that the SOC 3

report does not contain the detailed description of tests performed and the results of those tests. Consequently, distribution of the SOC 3 report is not limited. This makes this level of service particularly attractive to companies that share information with other business partners as part of their operations, but want to assure the public at large that their personal data is kept secure and confidential. For example, a large online retailer may establish an affiliates program that permits small retailers to use the transaction processing systems of the online retailer. Because of the concern that many customers of the small retailers may have regarding the online retailer's collection and use of purchase information, the online retailer and the small retailers wish to assure customers that the online retailer maintains the privacy of customers' information. Management of the online retailer may request a SOC 3 engagement, performed by a CPA over the system of processing using the Trust Services Principles and Criteria, and may then distribute the SOC 3 report to customers via a link on its website and publicly display the SOC 3 Report: SysTrust for Service Organizations seal.

Interestingly, although SSAEs are issued by the AICPA, management thereof chose not to address many of the data security issues within SSAE16. Instead they chose to separately draft and publish the SOC engagement guidelines. This facilitates the continued existence of a strong divergence between international and domestic service organization assurance, at least in practice. Presently, a large contingent still exists that believes that not enough is being done to stem the tide. An article published as recently as January 2012 states that "Audit standards have not yet developed to the point where there is clear-cut guidance to external auditors regarding how and what to test in a client's operations when these depend on a cloud service provider. The SOC standards only provide general guidance regarding the reliance of an external auditor on the attestation service provided by another independent accountant regarding a cloud provider's

assertions on selected aspects of their systems and operations" (Nicolaou, Nicolaou, & Nicolaou, 2012).

History of Cloud Computing

The concept of Cloud Computing was first introduced in the early 1960s, but the popularity of this internet paradigm has only blossomed within the past decade or so. Consequently, the bulk of the history is fairly recent. First a discussion of what constitutes cloud computing.

NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models. They are:

Essential Characteristics:	1) Broad Network Access 2) Rapid Elasticity 3) Measured Service 4) On-Demand Self-Service 5) Resource Pooling
Service Models	1) SaaS 2) PaaS 3) IaaS
Deployment Models:	1) Public 2) Private 3) Hybrid 4) Community

Essential Characteristics of Cloud Computing

Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches:

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloud-based software services.

Rapid elasticity: Capabilities can be rapidly and elastically provisioned — in some cases automatically — to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts). Resource usage can be monitored, controlled, and reported — providing transparency for both the provider and consumer of the service.

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage as needed automatically, without requiring human interaction with a service provider.

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a degree of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources

include storage, processing, memory, network bandwidth, and virtual machines. Even private clouds tend to pool resources between different parts of the same organization.

Cloud Service Models

Cloud service delivery is divided among three archetypal models and various derivative combinations. The three fundamental classifications are often referred to as the "SPI Model," where 'SPI' refers to Software, Platform, or Infrastructure (as a Service). These three components are defined as:

Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources

where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Although exact usage numbers reported vary somewhat, it is clear that all three cloud service models are experiencing strong growth. In their April 26, 2011 blog, *DataTrendsPublications* reports that "SaaS adoption is up 13 points over last year, to 60 percent" (DataTrendsPublications, 2011). Estimates for PaaS usage are currently somewhat nebulous, as best indicated by comments from Kamesh Pemmaraju of the Sand Hill Group. In his August 27, 2011 article "Let the Cloud Wars Begin: Who Will Be the Winners?", he states that "enterprise use of PaaS will be in its infancy" and that "Sand Hill's latest survey results bear this out: a *whopping 40 percent* of the respondents stated that they don't plan to use PaaS now or in the next 12 months" (Pemmaraju, 2011). This would indicate that 60% are, in fact using PaaS currently. Finally, in its report "Is IaaS Moving Beyond Just Cloud Fluff?", Yankee Group found that 24 percent of large enterprises with cloud experience are already using IaaS, and another 37 percent expect to adopt IaaS within the next 24 months (Hickey, 2010).

While multi-tenancy is not specified as an essential cloud characteristic by NIST, it is frequently discussed as such and it is therefore appropriate to include it here.

Multi-Tenancy: Multi-tenancy in cloud service models implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. Consumers might utilize a public cloud

provider's service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure. From a provider's perspective, multi-tenancy suggests an architectural and design approach to enable economies of scale, availability, management, segmentation, isolation, and operational efficiency; leveraging shared infrastructure, data, metadata, services, and applications across many different consumers. Multi-tenancy can also take on different definitions depending upon the cloud service model of the provider; inasmuch as it may entail enabling the capabilities described above at the infrastructure, database, or application levels. An example would be the difference between an IaaS and SaaS multi-tenant implementation. Cloud deployment models place different importance on multi-tenancy. However, even in the case of a private cloud, a single organization may have a multitude of third party consultants and contractors, as well as a desire for a high degree of logical separation between business units. Thus multi-tenancy concerns should always be considered (Brunette & Mogull, 2011).

Cloud Deployment Models

Service model notwithstanding, cloud services are typically deployed via one of four models. These are:

Public Cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Private Cloud: The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises.

Community Cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises. For example, all government organizations within a particular state may share computing infrastructure on the cloud relating to the citizens residing in that state. Another good example would be a group of medical facilities within a specific geographical region sharing computer infrastructure, as they all utilize the same patient-tracking software and must all meet the same HIPAA requirements.

Hybrid Cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Figure 1 provides an overview of the various components of the cloud computing environment, as it is currently defined.

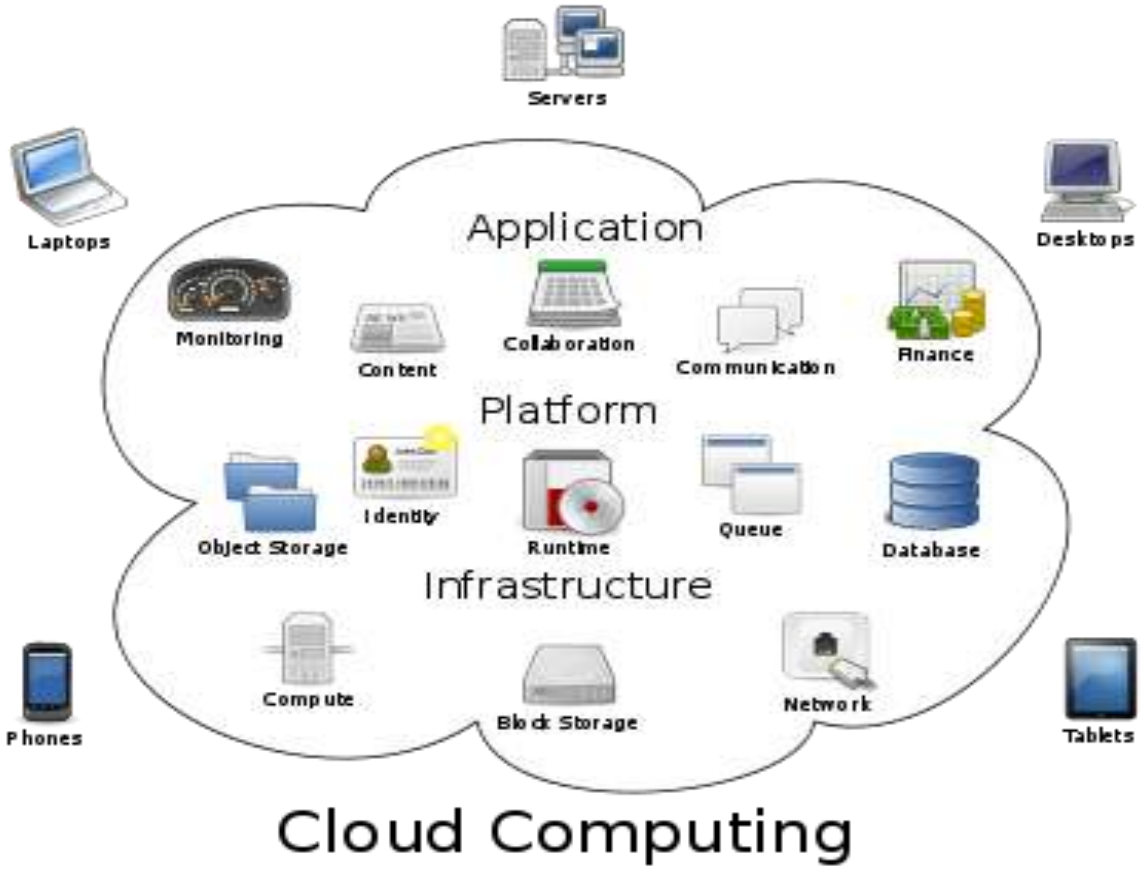


Figure 1 - Cloud Computing Environment[3]

Pros and Cons

The potential benefits of cloud computing are touted throughout the popular media and most people would have difficulty refuting the majority of the claims. Some of the more popular benefits are: quick implementation, anytime/anywhere access, lower upfront costs, little or no hardware or maintenance costs, reduced support costs, easier upgrades, disaster recovery and

[3] Created by Sasa Stephanovic

backup capabilities, etc. (DeFelice & Leon, 2010). But the cloud is not all gain and no pain. While the cloud offers all these advantages, until some of the risks are better understood, many of the major players will be tempted to hold back (Viega, 2009). Managers are fully aware that they are held responsible for the security and regulation of the data within their realm of influence, regardless of where it is located or who has physical control. They also understand that they have a fiduciary duty to protect not only the data that belongs to their company, but also the data obtained from outside parties as well. The PRC notes that it is virtually impossible for individuals to protect themselves from a data breach and that it is up to organizations that collect data on consumers to take the steps to ensure the privacy and security of the data they collect and maintain.

According to a recent IDC survey, 87.5% of IT executives and CIOs cited security as the top challenge in their adoption of the cloud services model, as compared to 74% in the prior year (Gens, 2009). This indicates that there is still a fairly strong concern among potential adopters regarding the security of the data that is placed in the cloud, and evidence suggests that some companies are still hesitant to participate. Seamus Reilly, director of IT risk advisory at Ernst & Young states "One of the perceived inhibitors in the uptake of cloud computing, particularly into the delivery of enterprise systems, is a need for assurance that there are controls operating to protect the confidentiality, integrity and availability of data and of their systems. Currently, recognized assurance standards do not fully address the wider requirements that cloud services bring." (Reilly, IT Management, 2011). In addition to the general security issues labeled confidentiality, integrity and availability of data, IT directors must specifically be concerned with answers to questions such as:

1. Do the vendor's employees look at my data while storing and processing it?

2. Can I view access logs and audit trails of all users and vendor employees to confirm no improper access is occurring?
3. Is my data truly safe from being co-mingled with someone else's data (if multi-tenancy is being utilized)?
4. Is my data always encrypted so that I'm protected even in the event of a data breach?
5. Are all of my compliance requirements being met? This is a particularly sticky problem because transfer of the "control" of the data and processing does not transfer the "responsibility" for regulatory compliance.
6. What happens if my third-party service provider is purchased by another company – perhaps my competitor? What happens if they go bankrupt?

This is not meant to be a comprehensive list of security issues facing IT directors – it is merely a sampling of the issues that must be addressed. However, based on just this brief list, is it any wonder that these IT professionals are leery of entrusting their company's future (and their own) to the cloud? Much of the current sentiment may best be expressed by Nicolaou et al., who state "It is currently unknown how providers will be able to protect data from theft and manipulation; therefore, organizations are only willing to place non-critical applications and general data in the cloud." (Nicolaou, Nicolaou, & Nicolaou, 2012)

Still, there are those that would disagree. In a recent write-up on the *Cloud Connect 2011* conference, Graham states "Security in the cloud has been a hot topic, but concerns seem to be waning as evidenced by the limited keynote and general session discussion focused on this issue" (Graham, 2011). She further opines that initial apprehensions about security, vendor lock-in, and data privacy are subsiding and new debates, such as public versus private/hybrid deployment, are

taking center stage. Still others point to the seemingly phenomenal revenue growth of the cloud industry as evidence that security issues are no longer a problem.

Growth

Analysts find that across industry, online collaboration and enterprise applications such as customer relationship management, supply chain management and enterprise resource planning drive the growth of cloud computing, and estimate that within the next five years, the global market for cloud computing will grow to $95 billion and that 12% of the worldwide software market will move to the cloud in that period (Subashini & Kavitha, 2011). A recent report by research firm Forrester estimates that the cloud computing market will leap from $41 billion in 2011 to more than $241 billion in 2020 with an annual growth rate of over 20%. Most of this growth is projected for the SaaS market, which is estimated to grow to $93 billion by 2016 and to $133 billion by 2020. Another major research firm, Gartner, estimates the cloud services market will exceed $148 billion as early as 2014. With its latest survey, Gartner received responses from 2,014 CIOs representing more than $160 billion in CIO IT spending and covering 38 industries across 50 countries. The survey found that only 3% of CIOs today have more than half of their infrastructure and applications operating in the cloud. But that number is expected to grow to 46% by 2015, making cloud transformation the hallmark of many CIOs at their current companies, and accounting for the phenomenal growth projected. Even the federal government is taking the plunge. The Office of Management and Budget (OMB) predicts that of the current $80 billion federal IT spending, $20 billion can potentially move to the cloud.

Prudent IT managers are risk averse when it comes to gambling the future of their companies and their careers. They look for assurance in order to mitigate potential risks before

making any major moves, and typically rely upon auditors to provide that assurance. Consequently, this is a perfect opportunity for auditors to maximize their contribution to the cloud computing movement. Gary Reiner, long-time CIO of General Electric was recently quoted as saying "As to any lingering security concerns, GE takes our security very, very seriously. We would never put virtual data outside the firewall unless it was secure." When asked how he knows for sure that GE's supplier data is secure outside his firewall, he says, somewhat ominously: "Audits." (Wailgum, 2009). The fact that his company spends $55 billion per year among its supplier base and that he has outsourced this function entirely, speaks volumes about the level of trust that he has in his third-party service organization and the assurance provided through them. But the most revealing part of his statement is the last word "Audits". Apparently, his trust is based primarily on the work of the third-party service provider auditors. If this is the level of faith being placed in the work of these auditors, it is incumbent upon all involved in the process to be worthy of such trust and respect.

But if auditors are doing such a good job of providing assurance on the security of data placed in the cloud these days, why is it that the number of data breaches continues to grow? If the guidance from SAS70, SSAE16, ISAE3402, and SOCs has proven so effective that companies are entrusting billions of dollars to the cloud based on that assurance, why are data stored in the cloud compromised on a daily basis? These are the questions that really must be addressed.

Recent Breach History

It was introduced earlier that cloud computing has actually been in existence since the 1960s, yet there is little history in the literature on breaches prior to the past decade or so. This

reality has several likely explanations. Development of the cloud much beyond the novelty stage only occurred during the past decade, so by virtue of a smaller presence in the past there would have been fewer breaches than experienced in more recent years. It is also possible that the breaches that did occur were simply not reported because current regulatory and societal pressures did not exist to encourage reporting of such events. It has typically been the view of managers that such things indicate weaknesses in the organization and should be kept quiet, lest the organization be somehow penalized for allowing such an occurrence.

In more recent years, there has been a substantial increase in breaches reported. The data used for this study from the Privacy Rights Clearinghouse provides the following descriptive data for the study period (2005 through 2011), which is provided in Table 1. Note that although observations date back to January 2005, the PRC did not start compiling this data until April 2005. Consequently, data from the first quarter of 2005 may be underreported.

Year	Number of Breaches	Number of Records
2005	136	52,821,610
2006	482	48,607,177
2007	452	129,974,978
2008	355	49,659,422
2009	253	218,903,225
2010	605	12,341,682
2011	564	30,760,879
Totals	2,847	543,068,973

Table 1 - PRC Descriptive Data

Although this reported number of breached records (> 543 million) may seem staggering for a relatively scant number of years, the director of the PRC, Beth Givens, says that this number is conservative. She continues "We generally learn about breaches that garner media attention. Unfortunately, many do not. And, because many states do not require companies to report data breaches to a central clearinghouse, data breaches occur that we never hear about. Our Chronology is only a sampling." (Privacy Rights Clearinghouse, 2011) Some of the more noteworthy 2011 breaches reported that are attributable to web-based exposure are:

1. Sony PlayStation (April 27) – Sony discovered an external intrusion on PlayStation Network (PSN) and its Qriocity music service on or about April 19th. Sony blocked users from playing online games or accessing services like Netflix and Hulu Plus on April 22nd. The blockage lasted for seven days. Sony believes criminal hacker(s) obtained names, addresses, email addresses, dates of birth, PSN/Qriocity password and login, and online IDs for multiple users. The attacker may have also stolen users' purchase history, billing address, and password security questions. Over the course of the next several months, Sony discovered that the hackers gained access to 101.6 million records, including 12 million unencrypted credit card numbers. This breach highlights the importance of password hygiene. Passwords are frequently the only thing protecting our private information from prying eyes. Many websites that store your personal information (for example web mail, photo or document storage sites, and money management sites) require just a user name and password for protection. Password-protected web sites are becoming more vulnerable because often people use the same passwords on numerous sites. One study by Sophos, a security firm, found that more than 30% of users recycle the same password for every site that they access.

In this case, the stolen passwords were unencrypted, meaning the criminal could potentially "break in" to other sites if the victims used the same password more than once.

2. Epsilon (April 2) – Epsilon, an email service provider for companies, reported a breach that affected approximately 75 client companies. Email addresses and customer names were affected. Epsilon has not disclosed the names of the companies affected or the total number of names stolen. However, millions of customers received notices from a growing list of companies, making this the largest security breach ever. Conservative estimates place the number of customer email addresses breached at 50 to 60 million. The number of customer emails exposed may have reached 250 million. Compromised email addresses and names may seem innocuous to some, but victims may fall prey to spear phishing. Spear phishing occurs when a criminal sends an email that sounds and looks like it's from a company the recipient has an account with because it addresses him or her by name. A spear-phishing message might say, "Hello Mr. Anderson, Because of the recent hacking incident affecting some Acme customers, we are asking you to visit this website [URL provided] and update your security settings." The email tries to convince trusting readers to "bite" on the bait and go to that website, and then divulge other information like Social Security numbers and credit card numbers. The result could be as serious as identity theft. What makes this breach so significant is that it highlights the risk of cloud-based computing systems and the need for greater cloud security measures.

3. Texas Comptroller's Office (April 11) – Information from three Texas agencies was discovered to be accessible on a public server. Sometime between January and May of

> 2010, unencrypted data was transferred from the Teacher Retirement Center of Texas, the Texas Workforce Commission (TWC) and the Employees Retirement System of Texas. It ended up on a state-controlled public server as early as April of 2010 and was not discovered until March 31, 2011. Sensitive information such as names, Social Security numbers, addresses, dates of birth and driver's license numbers could have been exposed. A spokesperson from the Texas Comptroller's Office claims that the breach occurred because numerous procedures were not followed. Some employees were fired for their roles in the incident. Approximately two million of the 3.5 million individuals possibly affected were unemployed insurance claimants who may have had their names, Social Security numbers and mailing addresses exposed. The birth dates and driver's license numbers of some of these people were also exposed. Two class action lawsuits have been filed on behalf of the 3.5 million Texans affected by the breach. One such lawsuit seeks a $1,000 statutory penalty for each individual, which would cost the state of Texas $3.5 billion if they lost and had to pay up. This breach is particularly significant because individuals generally do not have a choice when providing personal information to a government agency. It is therefore vitally important that government agencies act as responsible stewards of personal data.

This is merely a small sampling of electronic data breaches from the most recent year; enough additional data exists from just the past few years to fill numerous volumes. But these few examples are sufficient to clearly indicate that the problem is serious and can easily get worse without intervention.

Further evidence of the magnitude of the breach problem is provided by the Ponemon Institute 2011 survey. They surveyed 583 IT security practitioners in the U.S. with an average of

9.6 years of experience. More than half are employed by organizations with over 5,000 employees. Some of their findings are:

1. Organizations are experiencing multiple breaches. More than half of respondents (59 percent) say they have had two or more breaches in the past 12 months and 10 percent do not know. Approximately 90 percent of organizations have had at least one breach.
2. As a result of these multiple breaches, more than one-third (34 percent) of respondents say they have low confidence in the ability of their organization's IT infrastructure to prevent a network security breach.
3. Insufficient budgets are an issue for many organizations. Fully 52 percent of respondents say 10 percent or less of their IT budget is dedicated to security alone.
4. In the next 12 to 18 months, 47 percent say their organizations will increase the portion of their IT dollars spent on security to over half of their total IT budget.

For purposes of the current study, one of the most telling results illuminated by the Ponemon survey is that "Security breaches most often occur at off-site locations but the origin is not often known. Mobile devices and outsourcing to third parties or business partners seem to be putting organizations at the most risk for a security breach" (Ponemon Institute LLC, 2011). In this portion of their survey, 28 percent say that breaches occurred remotely and 27 percent say it was at a third party or business partner location.

Another 2011 analysis provides even more onerous results. Since the cloud concept was originally developed by the telephone companies, it is only appropriate that they still have a hand in moving it from concept to practice. For the past several years, Verizon® has, in conjunction with the U.S. Secret Service, been producing a *Data Breach Investigations Report*. The Verizon

2011 offering reveals some interesting statistics. The report states that "We constantly see breaches involving hosted systems, outsourced management, rogue vendors, and even virtual machines, though the attack vectors have nothing to do with it being a virtual machine or not. In other words, it's more about giving up control of our assets and data and not controlling the associated risk, than any technology specific to The Cloud" (Baker, Hutton, Hylender, Pamula, Porter, & Spitler, 2011). They report that half of the IT assets encountered during their investigation were fully or partly managed by a third party, and that overall, both hosting and management were a little more likely to be handled by external parties compared to prior years. Interestingly, they opine that the combination of outsourcing plus indifference and/or negligence with respect to vendor management—which is seen more often than people might think—is almost certainly a contributor (to the breach statistics). Some of the more enlightening statistics that they assert include:

1. 92% of data breaches stemmed from external agents (+22% from prior year)
2. 50% involved some form of hacking (+10% from prior year)
3. 92% of attacks were not highly difficult (+7% from prior year)
4. 76% of all data was compromised from servers (-22% from prior year)
5. 96% of all breaches were avoidable through simple or intermediate controls (no change from prior year)

These results seem to provide substantiation to the premise that the problem continues to grow, despite current efforts to combat it. And if the findings of this Verizon® report are to be believed, item 5 above indicates that the problem is largely preventable. If this is truly the case, this current research should prove valuable to those who intend to try to stem the tide. Whether fortunate or unfortunate, auditors are seen as the "information police" in the minds of most

educated individuals. The opportunity to be a large part of the solution is already thrust upon them – auditors just have to be willing to make the leap from protecting themselves to protecting their clients through enhanced job performance.

Cost of Breaches

Data breaches cost billions annually – of this there is little doubt. Although determination of a specific dollar figure is very difficult and estimates vary widely, nobody denies that it is a large and expensive problem. Interest in this problem has become so prevalent in business today that Darwin Professional Underwriters Inc., a Farmington, CT-based technology liability insurance company, has released a free online calculator that it said allows businesses to estimate – with a fair degree of accuracy – their financial risk from data theft. In his 2007 article in *Computerworld* magazine, Vijayan states:

> "Darwin's Data Loss Cost Calculator uses proprietary algorithms developed with security breach data from media reports and other industry resources, according to the company. Companies input data in the respective fields in the calculator to get instant estimates for costs associated with breach-related activities such as customer notification, credit monitoring, crisis management consulting, state or federal fines, and attorney fees. The calculator does not include costs associated with any class-action or other lawsuits that might follow a data breach, he said. Neither does it look at the effect on stock prices or reputation, because such numbers can vary by incident and are much harder to generalize." (Vijayan, 2007)

The financial consequences of a security breach can be severe. When asked to consider cash outlays, internal labor, overhead, revenue losses and other expenses related to the security breach, 41 percent of respondents reported that it was $500,000 or more and 16 percent said they were not able to determine the amount. This estimate about the cost is consistent with two other studies Ponemon Institute conducts annually: the Cost of a Data Breach and the Cost of Cyber Crime. According to those findings, the average cost of one data breach for U.S. organizations participating in the 2010 study was $7.2 million and the average cost of one cyber attack for U.S. organizations participating in the 2010 study was $6.4 million (Ponemon Institute LLC, 2011).

Cloud-specific Breach Issues

Some readers might assume that all assurance services that fall under the SAS70, SSAE16, ISAE3402, and SOCs umbrella would be cloud-specific. After all, these guidelines are all specific to audits of third-party service providers. However, as has been illuminated in the previous sections, with the exception of SOC Type 2 and SOC Type 3 engagements, the primary focus of all this guidance is specific to controls over data used in financial reporting. Yet much of the assurance that is sought by businesses in the current markets relates to concerns of a non-financial nature. Also, many arrangements still exist between providers and consumers of "off-site processing and data storage" services that do not qualify as cloud computing. Nevertheless, the bulk of what has been discussed thus far and in fact the bulk of what is currently being written in the literature about third-party service provider assurance concerns cloud computing.

Providing security in the cloud presents some new challenges for many organizations. Current cloud offerings are essentially provided via public (as opposed to private) networks, which presumably expose them to more attacks. There are also requirements for auditability that

must be met, to ensure compliance with legislation such as the Sarbanes-Oxley Act and the Health and Human Services Health Insurance Portability and Accountability Act (HIPAA). These Acts establish security procedures that must be provided for in order to move corporate data to the cloud. Some researchers believe that there are no fundamental obstacles to making a cloud-computing environment as secure as the vast majority of in-house IT environments, and that many of the obstacles can be overcome immediately with well-understood technologies such as encrypted storage, Virtual Local Area Networks, and network middleboxes (e.g. firewalls, packet filters). For example, encrypting data before placing it in a Cloud may be even more secure than unencrypted data in a local data center. This is one of the recommendations most frequently made by security professionals, but as indicated in the Verizon® paper (and others), seems to be grossly underutilized, which is surprising, since it is also one of the least expensive methods of achieving data security. One scholarly offering is that auditability could be added as an additional layer beyond the reach of the virtualized guest OS (or virtualized application environment), providing facilities arguably more secure than those built into the applications themselves and centralizing the software responsibilities related to confidentiality and auditability into a single logical layer. Such a new feature reinforces the Cloud Computing perspective of changing the focus from specific hardware to the virtualized capabilities being provided (Armbrust, et al., 2009).

Legal issues must also be considered by managers contemplating a move to the cloud. Many nations have laws requiring SaaS providers to keep customer data and copyrighted material physically housed within national boundaries. But most companies would probably prefer not to have their data subject to the whims of the national political parties. Few businesses would be happy with the ability of a country to get access to their data via the court system; for

example, a European customer might be concerned about using SaaS in the United States given the U. S. Patriot Act, which allows legal access to private data under certain circumstances. The current trend among cloud service providers is to offer choices to consumers to alleviate these problems. For example, Amazon provides services located physically in the United States and in Europe, allowing providers to keep data in whichever location they choose. This gives businesses the ability to expand their consumption as their needs change. If they desire new services in a new location, it can be accomplished with a simple configuration change, avoiding the need to find and negotiate with an overseas hosting provider.

One recently proposed cloud assurance service offering that may hold promise is the concept of "Risk Assessment as a Service". In their 2010 working paper, Kaliski and Pauley suggest that traditional assessments developed for conventional IT environments do not readily fit the dynamic nature of the cloud. As an alternative, they propose a cloud-based assessment paradigm that would rely on an autonomic system that is reactive and proactive to its environment. (Kaliski & Pauley, 2010). Another recent study examines the information assurance practices of vendors based on their traffic volume, company size and service offerings (Chakraborty, Ramireddy, Raghu, & Rao, 2010). In just the past few years several cloud computing initiatives have been established to address cloud information assurance practices. These include CloudAudit, the Cloud Security Alliance, the Open Cloud Manifesto, the World Privacy Forum's Cloud Privacy Report, and Shared Assessments.

CloudAudit is actually a tool, designed to provide a common interface and set of processes and technologies to enable cloud service providers to automate the collection and assertion of operational, security, audit, assessment, and assurance information. Originally developed as the foundation of a stand-alone organization by C. Hoff of Cisco Systems, it was

incorporated into the Cloud Security Alliance (CSA) in October of 2010 (Subramanian, 2010). According to their website, the CSA is "a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders." (Cloud Security Alliance, 2011). Formally established in December of 2008, this organization has grown quickly and now has members from most of the leading service providers in the cloud computing industry, as well as many of the larger consumer organizations. In 2009, the Open Cloud Manifesto was released, and subsequently an organization grew out of it. The manifesto itself is merely a stated list of core principles by which cloud services should be developed and offered for consumption. There was much controversy surrounding the release of this document, as some of the larger players – i.e., Google and Microsoft, stated they were not allowed input into the document but were asked to sign in support of it. To date, they have both declined. The stated goal of this organization is to "ensure that organizations will have freedom of choice, flexibility, and openness as they take advantage of cloud computing." (Open Cloud Manifesto, 2011). The underlying premise is to protect consumers – particularly the smaller and less powerful ones, from the industry giants who possess the ability to dominate the industry and dictate the rules of pricing and service levels. The World Privacy Forum, founded in 2003, has also joined the "consumer protection" proponents in the cloud computing arena. In 2009 they released a report titled "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing", that addresses the privacy rights that consumer organizations may unwittingly be ceding when opting to outsource some business functions (Gellman, 2011).

The surge in movement to the cloud environment also inspired the creation of organizations like Shared Assessments. This organization's focus is based on the perceived "need for a standardized and objective vendor management assessment methodology that would help outsourcers meet regulatory and risk management requirements while significantly reducing costs for all stakeholders." (Shared Assessments, 2011) This program was originally developed by Bank of America Corporation, The Bank of New York Mellon, Citi, JPMorgan Chase & Company, U.S. Bankcorp, and Wells Fargo & Company in collaboration with leading service providers and the Big 4 accounting firms, and was launched in 2006. Consequently, its focus appears to be more consumer-side driven.

Considering the growth in the formation of third-party service providers offering cloud services and the level of attention being attracted in the media by the "cloud phenomenon", it is incumbent upon accounting academia to provide empirical research to investigate the adequacy of the current efforts being made to provide the desired level of assurance on the internal controls employed by these organizations. It is the goal of this research to enhance that investigation by examining the impact that security-focused attest services provided to third-party service providers may or may not have, when measured by the incidence of data breaches. This research also seeks to determine what factors influence the decisions made by IT directors and determine if they are relying on the right information to make those decisions.

Chapter III

METHODOLOGY

This research is designed to address the issue of data breaches, particularly as they are related to electronic activities. It will empirically establish that a significant trend does exist in breach frequency over time. It will also establish that the threat level posed by data breaches varies significantly by type of breach and type of organization, and will identify significant relationships between breach type(s) and organization type(s) to assist auditors in the risk assessment portion of their engagement planning. An additional objective is to empirically determine if SAS70/SSAE16/SOC audit services and/or prior breach exposure affect the decisions of CIOs regarding their consideration of whether to employ cloud/datacenter-hosted solutions. Also, it will determine if CIOs are educated in the different levels of IT certification to determine if the audit profession is providing sufficient education on the subject. The following research questions have been developed to address these goals:

1. Are there any significant anomalies in reported breach data that could be used to benefit auditors?
2. If type of organization is significantly associated with type of breach, which organization types are most vulnerable to which types of breaches?

3. Do any of the following influence CIOs when making outsourcing (cloud) decisions?

    Prior breach experience
    Level of importance placed on audit certification
    Level of personal knowledge of assurance levels

Research Design

Exporting key business data and processes into the cloud computing environment is rapidly becoming a business imperative. In order to maintain a competitive edge, businesses must always try to, at a minimum, "keep up" with the competition. But as the move into the cloud has gained momentum over the past decade, this data model has become the norm rather than the exception. Cloud vendors and cloud consumers both extol the virtues and downplay the shortcomings. The high current level of interest in the cloud benefits this research, as the topic is very popular and current. Much is being written on the topic with new articles appearing almost daily, yet little of it is empirical in nature. Most is published from an IT marketing perspective (and predominantly web-published), with little empirical support. The intent of this study is to add validity to the current body of knowledge in this area through proper data selection and testing in order to confirm and/or refute some of the current claims and beliefs.

The research will be performed in two separate phases. The first phase of the study will utilize available data on the frequency and type of data breaches experienced by various types of organizations. This data, taken from the Privacy Rights Clearinghouse website, will be analyzed using standard statistical analysis techniques, such as cluster analysis, frequency analysis and binomial logistic regression. The second part of the study will utilize data obtained from a survey administered to 67,749 IT directors located throughout the U.S. This data will also be

analyzed using multiple statistical analysis techniques, including Chi-squared tests and binomial logistic regression.

Sample

As noted above, the first part of this study will use data from the Privacy Rights Clearinghouse database. The Privacy Rights Clearinghouse is a non-profit organization that compiles information on reported data breaches from a multitude of sources. This data has been collected since April of 2005 and is updated approximately every two days. This data will be sorted in numerous ways so that the necessary comparisons can be made and statistical analyses performed in order to address the hypotheses. The sample period under investigation, 2005 through 2011, contains 2,847 breaches affecting 543,319,784 individual records. The data were first analyzed for the purpose of providing guidance to auditors regarding the existence of any: seasonal component(s), overall frequency by breach type, overall frequency by organization type, and relationships between breach type by organization type.

The types of data breaches to be investigated are constrained by the classification of the data in the Privacy Rights Clearinghouse database. Consequently, analysis of breaches will be confined to the categories dictated by the data source. Specific identification of all breach types and their respective descriptions are presented below.

Variables

Breach-type variables (Dichotomous)

DISC – Unintended Disclosure: Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.

HACK – Hacking or Malware:	Electronic entry by an outside party, malware and spyware.
CARD – Payment Card Fraud:	Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
INSD – Insider:	Someone with legitimate access intentionally breaches information - such as an employee or contractor
PHYS – Physical loss:	Lost, discarded or stolen non-electronic records, such as paper documents
PORT – Portable device:	Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.
STAT – Stationary device:	Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility
UNKN – Unknown	

Other important categories related to data breaches also exist, for example: provider downtime, provider system crashes, data lost in cyberspace, and vendor lock-in, but they are not addressed in this research due to the unavailability of comprehensive and reliable data sources for these issues.

Also due to the constraints imposed by the data source, organization types will be limited to the following:

Organization-type variables (Dichotomous)

BSO – Business, Other

BSF – Business, Financial & Insurance

BSR – Business, Retail/Merchant

EDU – Educational Institutions

GOV – Government/Military

MED – Medical/Healthcare Providers

NGO – Nonprofit Organizations

Additional variables necessary for and used in the analysis of the data set are:

Other variables

BRCH_TYP – Categorical variable that indicates breach type (1 through 8)

MON_YR – Nominal variable that indicates the month/year of the breach

ORG_TYP – Categorical variable that indicates organization type (1 through 7)

All 2,847 breach incidents reported for the period under review were used in the analyses conducted for research questions 1 and 2.

Research question 3 was addressed using the results of the email survey conducted. The survey was sent to 67,749 IT directors at organizations throughout the U.S. Unfortunately, the database used for this phase of the research proved to be less reliable than was anticipated. Of the 67,749 emails transmitted, there were 23,624 that were returned as undeliverable, leaving an initial sample of 44,125 "delivered" surveys. Sadly, only 203 responses were received, and many of them were only partially completed. This represents a survey response rate of approximately ½ of 1 percent, after eliminating the undeliverable emails. Variables established for the analysis of the survey are:

AUD_PR_BRCH	If prior breach was with an audited CSP, 1; otherwise 0 (also from survey questions 4a and 4b)
AUDIT_IMPT	Level of importance placed on certification of CSP (survey question 6)
CSP_AUDITED	If current Cloud Service Provider (CSP) is audited, 1; otherwise 0 (survey question 3)
INTENT	If still willing to outsource, 1; otherwise 0 (survey question 5)

KNOW	Knowledge of differences in assurance levels provided (survey question 7)
PRIOR_BRCH	If prior breach experienced, 1; otherwise 0 (survey questions 4a and 4b)
USE_CLOUD	If currently use cloud, 1; otherwise 0 (survey question 1)

The conceptual model presented in Figure 2 below will help explain the intent of this portion of the study and identify the important relationships that are under examination.

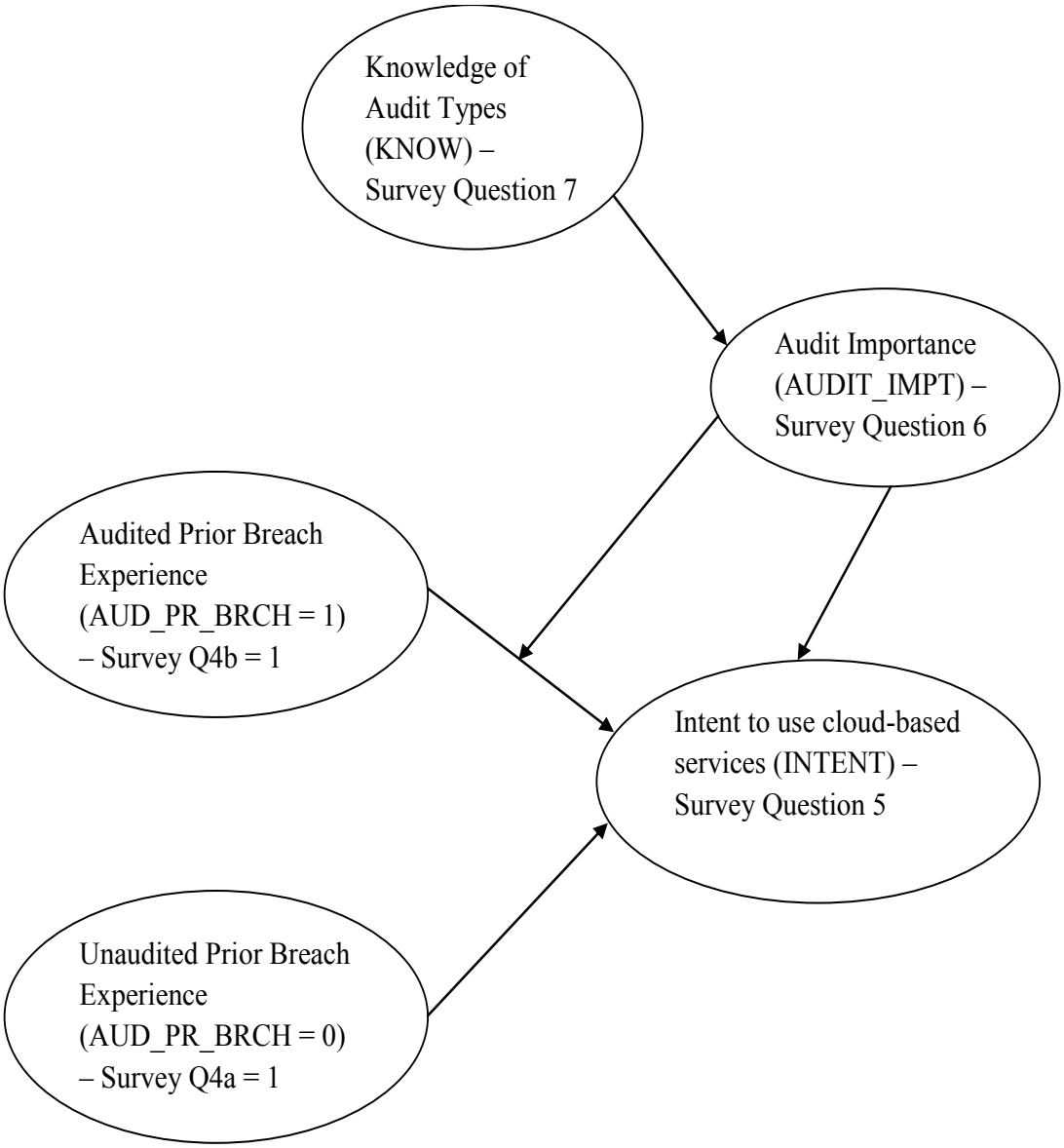


Figure 2 –Conceptual Model for Research Question 3

This conceptual model can be represented by and will be examined using the following regression equation:

$$INTENT = \beta_0 + \beta_1(AUDIT\_IMPT) + \beta_2(AUD\_PR\_BRCH) + \beta_3(PRIOR\_BRCH) + \beta_4(AUD\_PR\_BRCH * AUDIT\_IMPT) + \varepsilon$$

Hypotheses

Addressing research question 1 requires a broad analysis of the data breaches both in the aggregate and separately, in order to identify trends in the data that could be exploited to the benefit of auditors. Procedures will be conducted to detect anomalies specific to: overall breach frequency as a function of time, breach type as a percent of total breaches, organization type as a percent of total breaches, and breach type by organization type. Trends are easy to spot visually by graphing the frequency analysis, so this is the first approach taken. Hypotheses 1 is based on the results of the previously cited recent surveys and popular media, which indicate that the frequency of data breaches is continually trending in an upward direction. This leads to:

H_1: There is a significant positive growth trend in overall breach frequency as reported by month.

Hypothesis 2 is also grounded in the popular media and recent surveys, both of which imply that certain breach types are more prevalent and/or more frequently reported as a concern among CIOs, giving:

H_2: There is a significant difference in reported breach frequency by breach type.

Hypothesis 3 is derived logically from the fact that different organization types possess differing levels of what would be considered readily exploitable information. For example, manufacturing entities would be unlikely to have nearly the number of electronic assets available for exploitation – i.e. personal and/or financial information, as would an entity in the financial services sector. Therefore, it is reasonable to expect that breach types that focus on this type of exploitation would also focus on those organization types in possession of such assets and/or electronic records. This defines Hypothesis 3 as:

H_3: There is a significant difference in reported breach frequency by organization type.

In addition to the aforementioned frequency-graphing technique, Chi-square tests and binary logistic regressions will also be performed for Hypotheses 1 through 3 to statistically confirm or deny the existence of any noted anomalies. Those findings that are statistically significant will be subjected to detailed analysis in Chapter IV; the insignificant findings will only be summarized there, with the bulk of their reporting relegated to the appendices.

The analysis of breach frequency by organization type warrants a more thorough dissection due to the potential importance it may represent, as it could provide a specific tool to be used by auditors. Therefore, research question two will endeavor to determine if there is a significantly higher incidence of breach associated with any specific pairing of breach type and organization type. This information could substantially improve the efficiency of audits by allowing auditors to focus their resources on detecting and preventing specific breach types, depending on the organization type of their client. As in the first three hypotheses, a visual analysis of a frequency graph will be performed. This will be followed by examination of a cluster analysis on the breach type variable versus the organization type variable. This is done to group similar observations, which will potentially lessen the volume of work imposed in the audit planning process. Based on this goal and fashioned in accord with Hypotheses 2 and 3, Hypothesis 4 becomes:

H_4: There is a significant difference in frequency of breach occurrence based on the combination of different pairings of breach types with organization types.

Research question three seeks to answer multiple questions, namely: a) if prior breach experience has any effect on the current outsourcing decision, b) if certification level impacts the

current outsourcing decision, and c) if personal knowledge of assurance levels impacts the current outsourcing decision. Given that surveys of CIOs consistently find that security is one of the topmost concerns regarding outsourcing, the logical assumption would be that CIOs have prior history with security breaches and will therefore be more risk-averse. A natural secondary effect to increased risk-aversion is typically an increase in the requirement for assurance from third-parties. These issues lead to Hypothesis 5, which states:

H_{5a}: Those with prior breach experience as measured by PRIOR_BRCH will exhibit a less positive attitude toward future outsourcing, as measured by their future outsourcing intent (INTENT).

H_{5b}: Given that prior breach experience exists (PRIOR_BRCH=1), there will be a greater likelihood of future outsourcing, as measured by future outsourcing intent (INTENT) for those whose prior breach (AUD_PR_BRCH) was of an unaudited nature.

Hypothesis 6 is designed to determine if decision-makers who choose to outsource business functions to the cloud actually place any importance on the assurance offered by SAS70/SSAE16/SOC audit reports on third-party service providers. Stated in the null, it reads:

H_6: There is no difference in future outsourcing intent (INTENT) based on level of importance placed on certification (AUDIT_IMPT).

Finally, Hypothesis 7 investigates if decision-makers are aware of the differences between the assurance levels provided by SAS70/SSAE16/SOC type reports versus SOC Type 2 and Type 3 audits, the latter being the only type that actually provide assurance specific to non-financial reporting goals. Given the continual media barrage regarding the complexity and importance of data security issues, it is expected that CIOs would be current on the issue and be aware of the

differences in audits so that their outsourcing decisions are based on the proper information. This is examined through Hypothesis 7, which reads:

H_7: There will be a significantly higher proportion of survey respondents who indicate that they are familiar with the differences in certification levels (KNOW = 1) than those who indicate that they are not familiar with the differences (KNOW = 0).

Tests

The following procedures are designed to identify and quantify these important relationships. It is acknowledged that other important categories of the source of data breaches also exist, for example: provider system crashes and data lost in cyberspace, but they are not addressed in this research due to the unavailability of a comprehensive and reliable data source for breaches attributable to these causal factors.

Testing of Hypothesis 1 will be accomplished by graphing the frequency analysis of the breaches over time variable (MON_YR). This will provide a visual analysis to aid in the identification of any overall trend in breaches, should one exist. Next, a Chi-squared statistic will be computed to determine if there is a statistically significant difference between the actual breach frequency observed and the expected breach frequency based on random ordering of the data. Should any relationship be detected, the visual analysis and Chi-squared testing will be repeated for each breach type individually, in an effort to specifically identify which breach types are most responsible for the trend.

Hypothesis 2 will also utilize a graphical representation of a frequency analysis. The evaluation in this case will be of the frequency of each breach type (BRCH_TYP) observed as a percent of total breaches. This is done in an effort to determine visually if there appear to be any

anomalies of frequency by breach type. Again, a Chi-square statistic will be employed to determine the statistical significance of any relationship(s) observed. This procedure will identify whether any particular breach type(s) constitute a significant portion of the total reported breaches.

Hypothesis 3 will be analyzed in similar fashion to Hypothesis 2, but the focus will be on whether particular organization types report breaches overall at a significantly higher rate than other organization types. Statistical analysis performed will mirror those used in the testing of hypothesis 2. This procedure will identify whether any particular organization types constitute a significant portion of the total reported breaches.

While the specific magnitude and direction of the relationship between data breach type(s) and organization type(s) has not previously been quantified, a prudent person would acknowledge the likelihood of the existence of a relationship between these two variables. Quantification of this relationship is important in that it may help identify the most prevalent breach types and the organization types most vulnerable to those breaches. Specific identification of these factors could lead to more efficient audit procedures by allowing auditors to more clearly focus their efforts and audit resources, and may even help mitigate future breaches. For that reason, the analysis of the frequency of each pairing of breach type by organization type warrants deeper examination, due to its potential importance. Testing for research question 2 will therefore be designed to determine if there is a significantly higher incidence of breach associated with any specific pairing of data breach type and organization type. To achieve this goal, Hypothesis 4 will be approached through multiple analyses. First, association between the two variables will be evaluated to confirm or deny the existence of a relationship between BRCH_TYP and ORG_TYP. A *Phi coefficient* variant of the non-

parametric Chi-square correlation statistic will be evaluated, which is deemed to be the more appropriate correlation-type statistic to use when the variables are both nominal.[4] Next, a frequency graph will be examined for each organization type by all breach types, to help identify possible significant combinations. Then, a cluster analysis will be performed on BRCH_TYP versus ORG_TYP, to further consolidate any relationships into more manageable groups.

Research question 3 constitutes the second portion of the research, which seeks to address issues of a slightly different nature and in a different manner, using data from a different source. Consequently, testing for Hypotheses 5 through 7 will be based on the data obtained from the survey that was conducted. These hypotheses are designed to indicate the level of importance IT decision-makers place on certain outsourcing criteria. More specifically, Hypothesis 5a will examine if prior breaches of any kind impact future outsourcing decisions. To accomplish this analysis, several data subsets must be created. First a subset must be created containing only those responses that replied "yes" to either of survey questions 4a and/or 4b (PRIOR_BRCH=1). This will limit cases in this group to only those that indicate they have experienced a breach of some sort in the past. Next, this subset must be further divided into two subsets: those that answered "yes" to survey question 5 (INTENT=1) and those that answered "no" (INTENT=0). The analysis for Hypothesis 5a will then be accomplished by running a Binary Logistic Regression (LOGIT) on these last two groups, which is appropriate for comparisons of sets of dichotomous variables. In this manner it can be determined if a statistically significant difference exists between the two groups. Hypothesis 5a predicts that there will be a difference.

Hypothesis 5b is designed to infer if there is a difference in future outsourcing intent based on audited CSPs versus non-audited, for those who have suffered a prior breach. The goal

[4] A Phi-coefficient is a product-moment coefficient of correlation and is a variation of Pearson's definition of *r* when the two states of each variable are zero and one. It was specifically designed for comparisons of dichotomous distributions – ie. each value is either yes/no, alive/dead, black/white, etc.

is to see if those that were previously "burned" by a breach, associate that outcome with the level of assurance they placed in the work of auditors. As in testing for Hypothesis 5a, a subset must be created that contains only "yes" responses to either of survey questions 4a and/or 4b (PRIOR_BRCH=1) in order to isolate only those having experienced some sort of prior breach. Testing will then be accomplished by conducting a non-parametric Chi-Squared test on the PRIOR_BRCH and AUD_PR_BRCH variables for this group. The specific test performed in this case is a McNemar's variation of the Chi-Squared test. It is most appropriate, because it is specifically designed to be applied to 2x2 contingency tables with a dichotomous trait, which is the case under examination here. It is also indicated for use when dichotomous variables are in use that also exhibit significant correlation.

Hypothesis 6 is designed to examine the level of confidence that IT decision-makers have in the assurance given by audit reports issued on third-party service providers, and the role it plays on their future outsourcing decisions. To accomplish this will require a comparison of the INTENT variable with the AUDIT_IMPT variable. A binary logistic regression test will be conducted, regressing AUDIT_IMPT on INTENT. This test is appropriate because the DV in the equation (INTENT) is dichotomous and the IV (AUDIT_IMP) is ordinal.

Finally, Hypothesis 7 seeks to determine if an IT director's level of understanding of the differences in assurance implied by the various auditor reports has an effect on his or her future outsourcing intent. This will be accomplished by comparing the future intent variable (INTENT) with the familiarity variable (KNOW). A simple binary logistic regression (LOGIT) will be used for this purpose.

In the analyses of Hypotheses 5 through 7 above, logistic regressions are conducted. Consideration was given to the use of loglinear analysis, since some authors would consider this

to be the method deemed most appropriate for use here because it works well for categorical response variables with more than two categories, which the classical form of logistic regression does not (Stevens, 2002). However, for purposes of this research, in those instances where LOGIT was employed, any categorical data under review was broken into dichotomous variables prior to performing any regressions, and therefore loglinear analysis was deemed unnecessary.

The expected results of this study were that there exist anomalies in the frequency of breaches both by breach type and by organization type. It was also expected that there are significant relationships between types of data breaches and the types of organizations that experience these breaches. It was further proposed that these relationships, once identified, can be exploited to aid in the conduct of examinations of third-party service providers in order to mitigate some of the breaches and perhaps build consumer confidence in the data security assurance provided by the audit process. It was also expected that certain criteria are more important to the decision to outsource critical business data and processes into the cloud than others. Identification of these important criteria should provide opportunities to focus audit resources on those areas considered most important to consumers. This survey investigation may also reveal an "education" problem in the accounting industry, whereby IT decision-makers are still unsure of the level of assurance being implied by the audit product in which they are placing their faith. Results of the procedures as outlined in this section are presented in the next section and will provide answers to these issues.

CHAPTER IV

RESULTS

This research was conducted with several goals in mind: to determine if any significant anomalies exist in reported data breach frequencies that could aid auditors, to empirically establish that the threat level posed by data breaches varies by type of breach and type of organization, to quantify the relationships between breach type and organization type, and to identify factors that affect the decisions of CIOs regarding their consideration of whether to employ cloud/datacenter-hosted solutions. As previously discussed, the data on breaches comes from the Privacy Rights Clearinghouse and contains information segregated into eight separate breach classifications. Statistical analysis of each of these eight categories reveals associations that could prove useful to auditors, so this section will present results of those analyses using all 2,847 observations contained in the full database.

Research Question One

Research question one asks whether there are any significant anomalies in reported breach data that could be used to benefit auditors.

The data was examined in a manner to detect relationships that might prove useful to auditors, including: overall breach frequency as a function of time, percent of total breaches assigned to each individual breach type, percent of total breaches borne by each organization type, and breach type by organization type. Results of these analyses indicate that factors do exist that could prove beneficial to auditors in the risk assessment phase of their engagement planning. Details of each analysis are provided below.

Addressing Hypothesis 1 begins with a visual inspection of the data. A timeline, displayed in Figure 3, displays one data point for each month/year, which yields 84 observations.

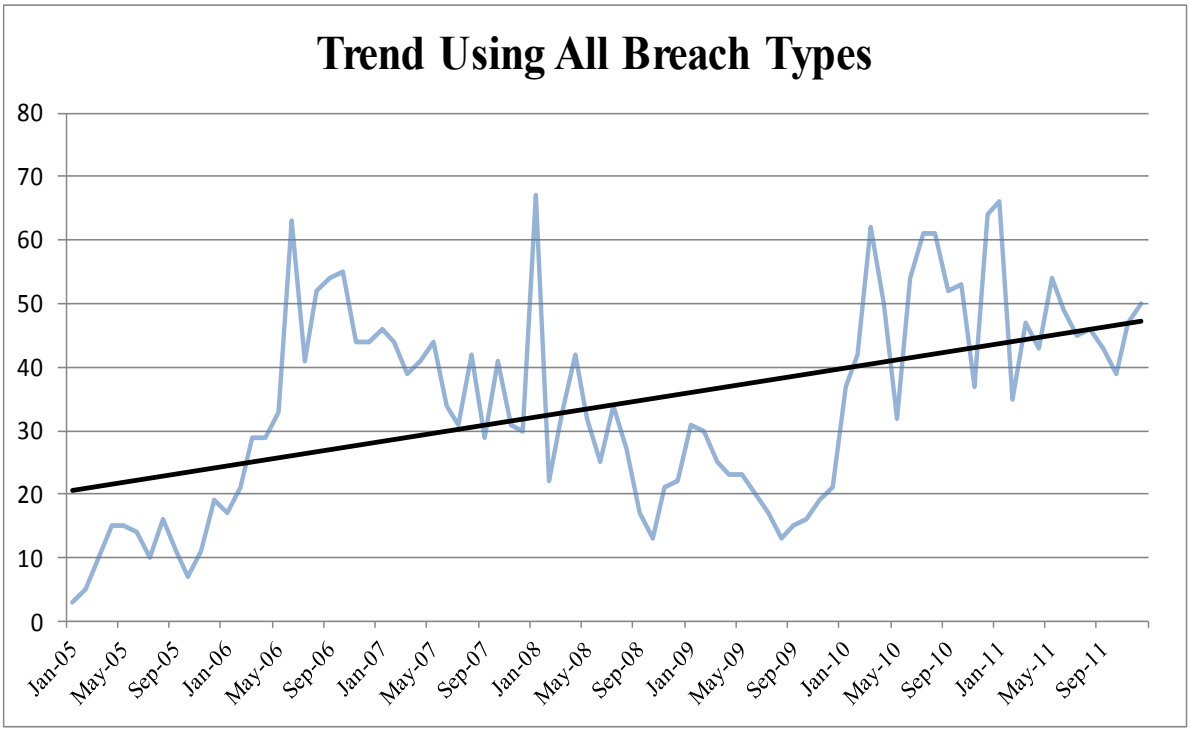


Figure 3 – Total Breaches Trend Analysis

The initial inspection of the data shows that there is a trend over time, providing support to the media hype that such is the case. Even though there are noticeable peaks and valleys evident

between months, the trend is clearly in an upward direction overall, as indicated by the superimposed linear trend line. This is further supported by the realization that there were only three breaches reported in January of 2005 and 50 reported in December 2011. So even on a simple linear basis, this represents a more than ten-fold growth in the number of reported breaches over just the past seven years. Confirmation that this pattern is statistically significant is provided by computing a Chi-squared test statistic. Significance for all the following tests is set at the level of $\alpha = 0.05$, unless otherwise specified. Presented in Table 2, this Chi-squared indicates a significant positive relationship (Phi = .560, p = .000 at the .05 level). The *Phi coefficient* is specifically targeted toward evaluations of nominal variables, as is the case here, and is therefore deemed the most appropriate test statistic (see footnote 4).

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	893.799	581	.000
Likelihood Ratio	912.531	581	.000
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.560**	**.000**
	Cramer's V	.212	.000
N of Valid Cases		2,847	

Table 2 – Significance Test of Breach Frequency Trend

Having established the existence of a significant growth trend, the logical next step is to attempt to identify if any particular breach types are more responsible for this trend. This

information could prove valuable, allowing auditors to address the "worst case" scenario(s) first. To that end, each breach type was then plotted individually over the 84-month period. This further analysis reveals that six of the eight breach types contribute at a significant level to the growth in the breach trend. The only two categories that are not statistically significant contributors to the overall growth trend are STATIONARY and UNKNOWN. Evidence of the significant breach types is presented in the following tables and graphs; the graphs and tables for the non-significant breach types are relegated to the appendices.

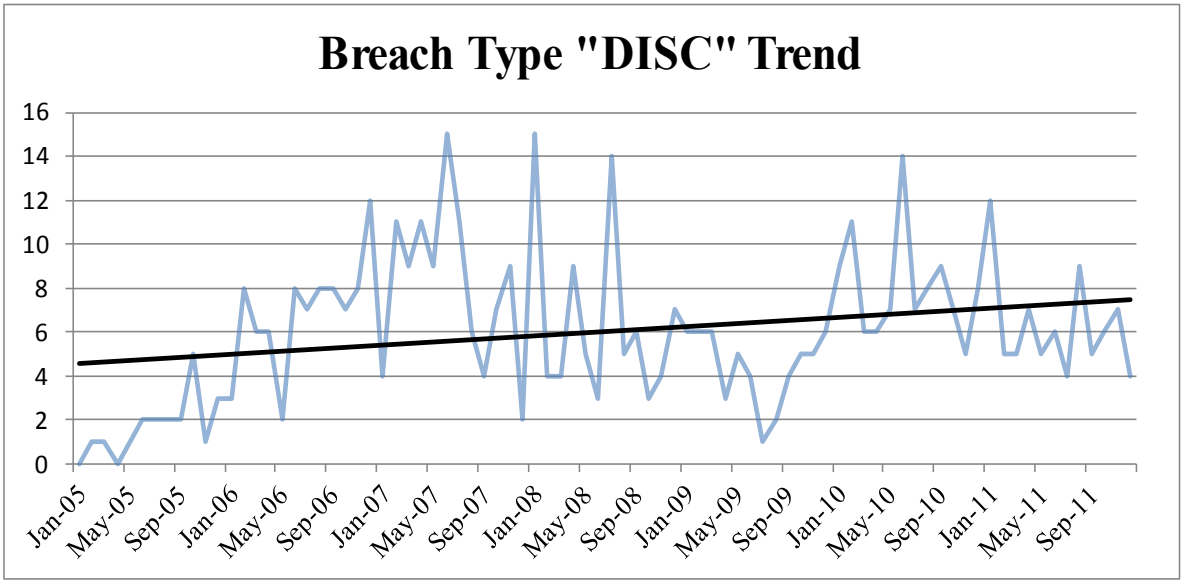


Figure 4 - "Unintended Disclosure" Trend

The positive association of the Unintended Disclosure (DISC) trend implied in figure 4 is confirmed to be significant in Table 3 by the *Phi coefficient* of .214 with a significant *p*-value of .001. This implies that reported breaches of this type have been rising at a significant rate since 2005. This could indicate that more persons are careless with the data that they control or simply that the reporting of this type of breach has become more prevalent.

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	130.317	83	.001
Likelihood Ratio	123.678	83	.003
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.214**	**.001**
	Cramer's V	.214	.001
N of Valid Cases		2,847	

Table 3 – Significance Test of "Unintended Disclosure" Trend

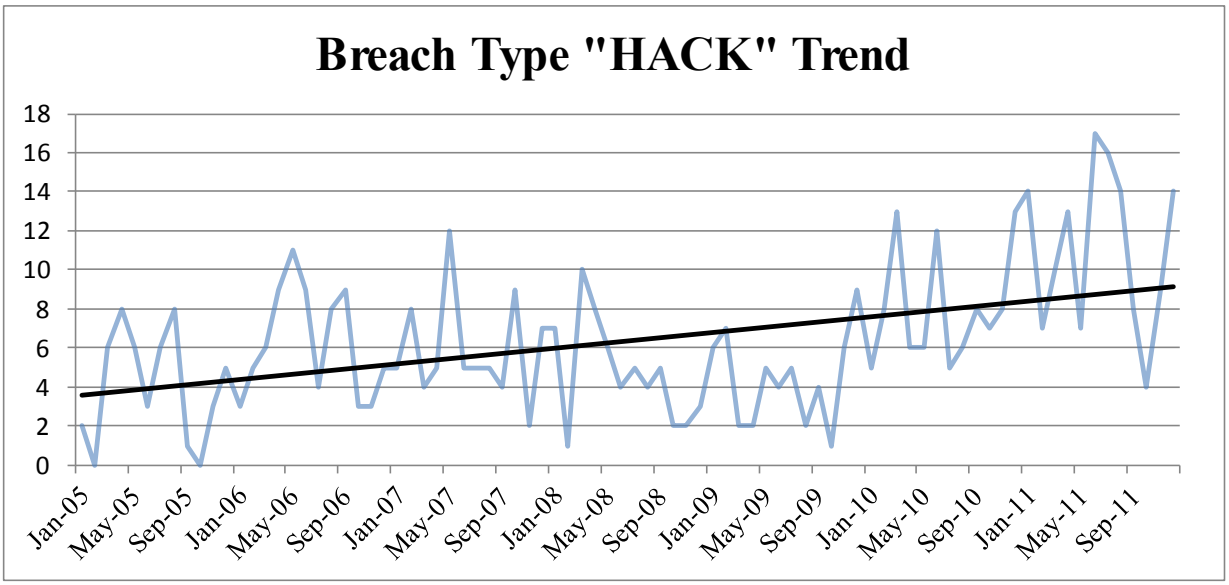


Figure 5 - "Hacking or Malware" Trend

The Hacking or Malware (HACK) breach type also demonstrates a positive association as evidenced in Figure 5, and it is confirmed to be significant in Table 4 (*Phi coefficient* = .243, *p* =

.000). Again, this confirms that reporting of breaches based on this classification has risen significantly since 2005. This could be indicative of an increase in available targets, a decrease in security diligence, or simply a heightened trend in breach reporting.

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	167.687	83	.000
Likelihood Ratio	159.928	83	.000
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.243**	**.000**
	Cramer's V	.243	.000
N of Valid Cases		2,847	

Table 4 - Significance Test of "Hacking or Malware" Trend

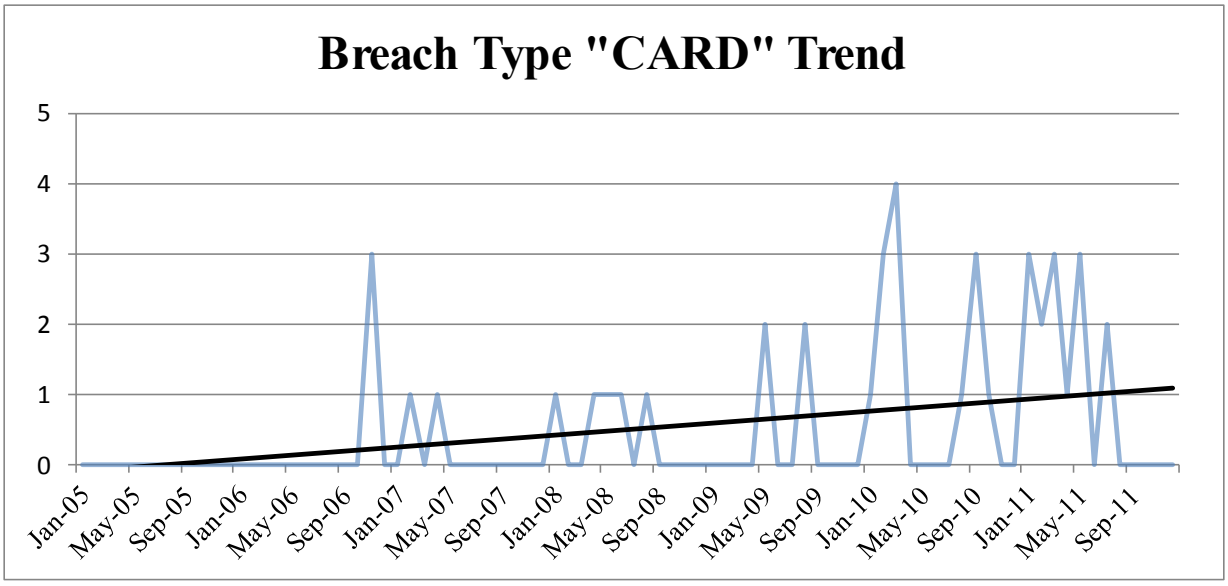


Figure 6 - "Payment Card Fraud" Trend

Without the superimposed linear trend line, Figure 6 would appear to suggest that no trend is present in the Payment Card Fraud (CARD) breach type. However, Table 5 indicates the existence of a significant positive association (*Phi coefficient* = .206, p = .004). Caution should be exercised in drawing any conclusion here due to the small sample size (41 observations) and the high number of cells containing 0 observations.

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	121.075	83	.004
Likelihood Ratio	103.195	83	.066
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.206**	**.004**
	Cramer's V	.206	.004
N of Valid Cases		2,847	

Table 5- Significance Test of "Payment Card Fraud" Trend

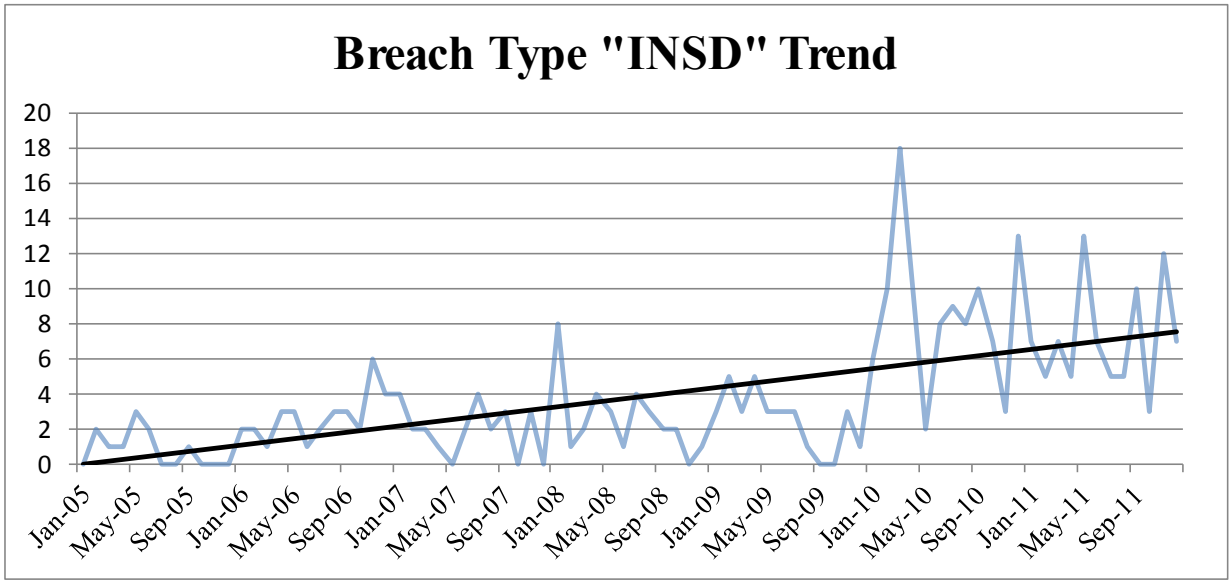


Figure 7 - "Insider" Trend

Similar to all those that precede it, breach type Insider (INSD) is also significantly and positively associated with the overall breach trend for the period under investigation. The statistics in Table 6 (*Phi coefficient* = .225, p = .000) confirm this assertion.

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	143.700	83	.000
Likelihood Ratio	161.423	83	.000
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.225**	**.000**
	Cramer's V	.225	.000
N of Valid Cases		2,847	

Table 6 - Significance Test of "Insider" Trend

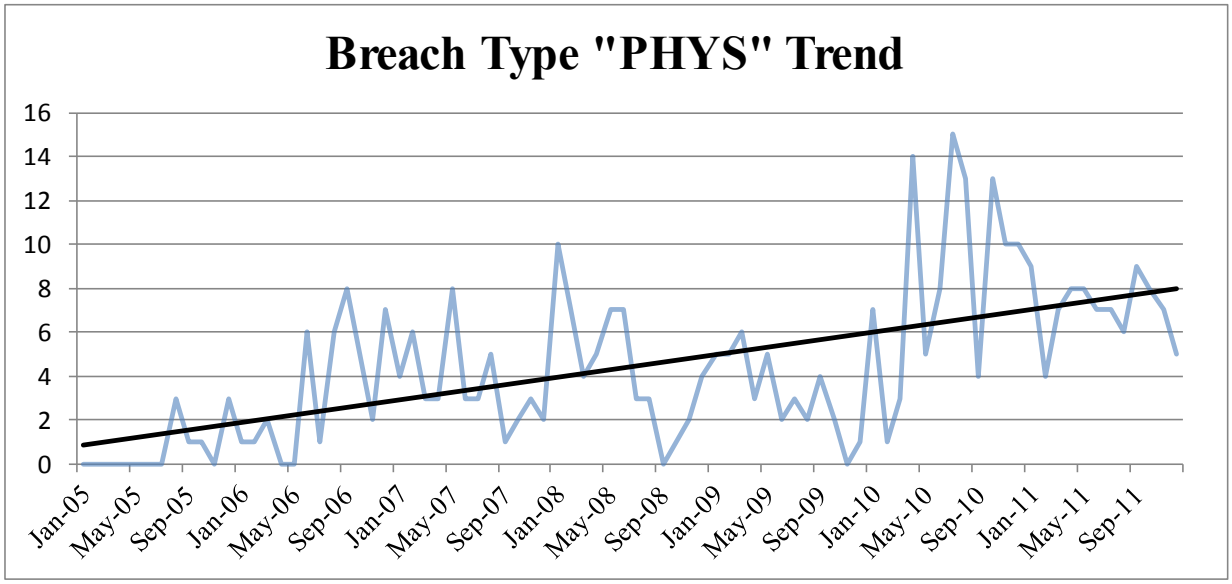


Figure 8 - "Physical Loss" Trend

The significance of the contribution of the Physical Loss (PHYS) breach type is fairly obvious and its positive significant contribution is borne out by the data in Table 7 (*Phi coefficient* = .212, p = .001).

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	127.472	83	.001
Likelihood Ratio	148.082	83	.000
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.212**	**.001**
	Cramer's V	.212	.001
N of Valid Cases		2,847	

Table 7 - Significance Test of "Physical Loss" Trend

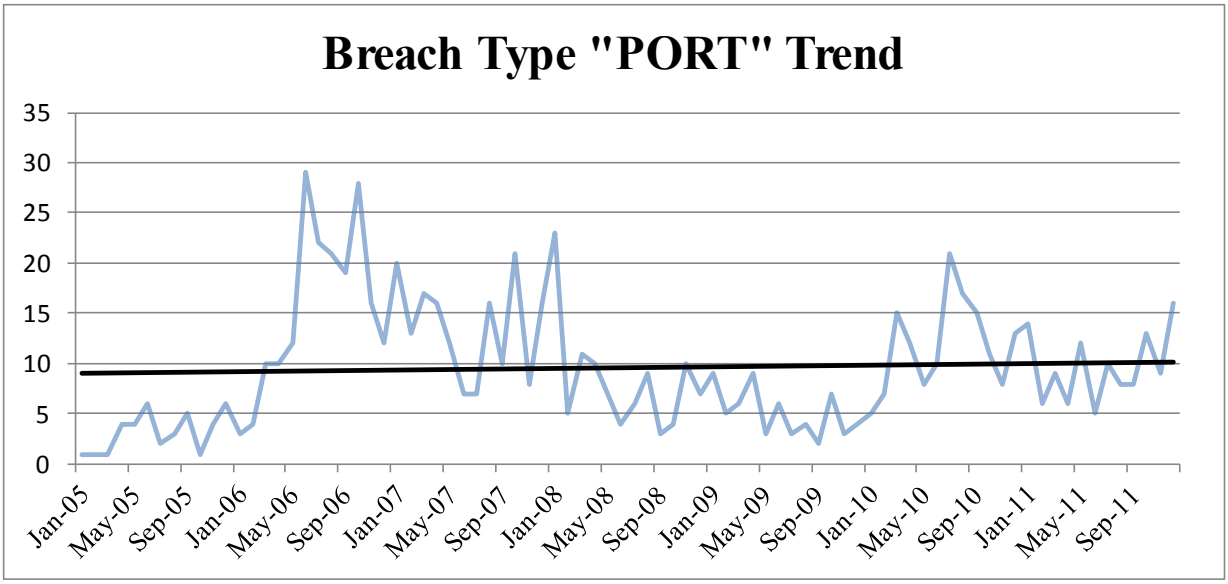


Figure 9 - "Portable Device" Trend

Figure 9 displays a graph that implies a positive growth in the Portable Device (PORT) breach trend, but the trend is so moderate that it is not easily translated into a significance level. However, the accompanying Table 8, does confirm a significant positive trend (*Phi coefficient* = .236, p = .000).

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	158.758	83	.000
Likelihood Ratio	157.966	83	.000
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.236**	**.000**
	Cramer's V	.236	.000
N of Valid Cases		2,847	

Table 8 - Significance Test of "Portable Device" Trend

Unfortunately, there is no clear "worst case" breach type trend, as was hoped. Consequently, this result provides minimal assistance to auditors in narrowing their focus. As previously disclosed, the last two breach type categories (STATIONARY and UNKNOWN) do not have a statistically significant relationship to the trend in the breach frequency as a whole, and are consequently not presented here. They are included in Appendix 6 for information purposes.

Of a more promising nature, the result from testing of Hypothesis 2 clearly indicates that certain breach types comprise a significant portion of the total reported breaches. Figure 10 reveals that almost 65% of all breaches fall into just 3 of the 8 categories.

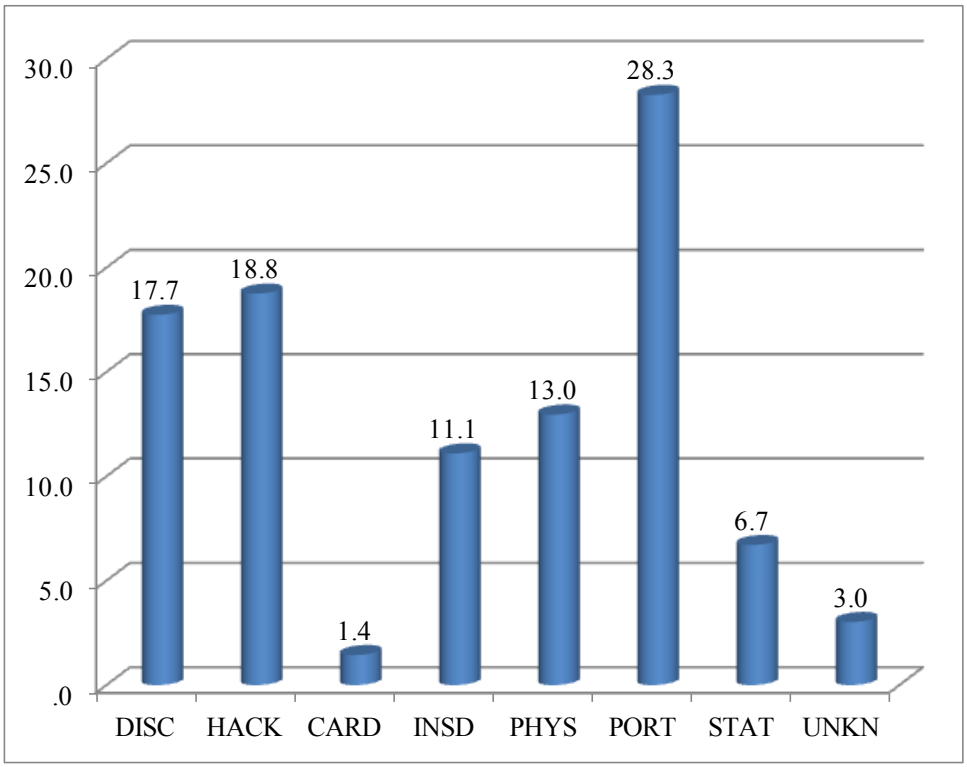


Figure 10 – Percent of each Breach Type of Total Breach Frequency

Further evaluation of this anomaly is accomplished through computation of a Chi-squared statistic to determine if the actual data dispersion differs in a statistically significant manner than

what would be expected. These results are presented in Table 9 below and indicate that the difference is significant. Note a. confirms that all cells have at least 5 observations, which strengthens the result.

Test Statistics

	BRCH_TYP
Chi-Square	1283.048[a]
df	7
Asymp. Sig.	.000

a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 355.9.

Table 9 – Significance Test of Total Breach Frequency by Breach Type

The importance of this information lies in the recognition that the three breach types representing the largest percentage of total breaches comprise 64.8% of all reported breaches. This knowledge alone is valuable to auditors seeking to maximize their limited resources when trying to combat the data breach problem. Efforts should be allocated first to breaches of the Portable Device group, then the Hacking or Malware group and then the Unintended Disclosure type. Addressing only these three types should provide assurance against roughly two-thirds of all breaches. On the other hand, breach types Stationary Device, Unknown and Payment Card Fraud only comprise 11.1% of total reported breaches. Auditors should allocate resources to these areas sparingly, as the return on investment would appear to be small.

Hypothesis 3 testing indicates that certain organization types experience breaches at significantly higher rates than the mean (14.2%), as presented in Figure 11. As seen here, over 60% of all data breaches are borne by only 3 of the 7 organization types. The data indicate that auditors of organization types Educational Institutions, Medical/Healthcare Providers, and

Government/Military should place a higher level of importance on the possibility of data breaches than organizations in the other four organization types.

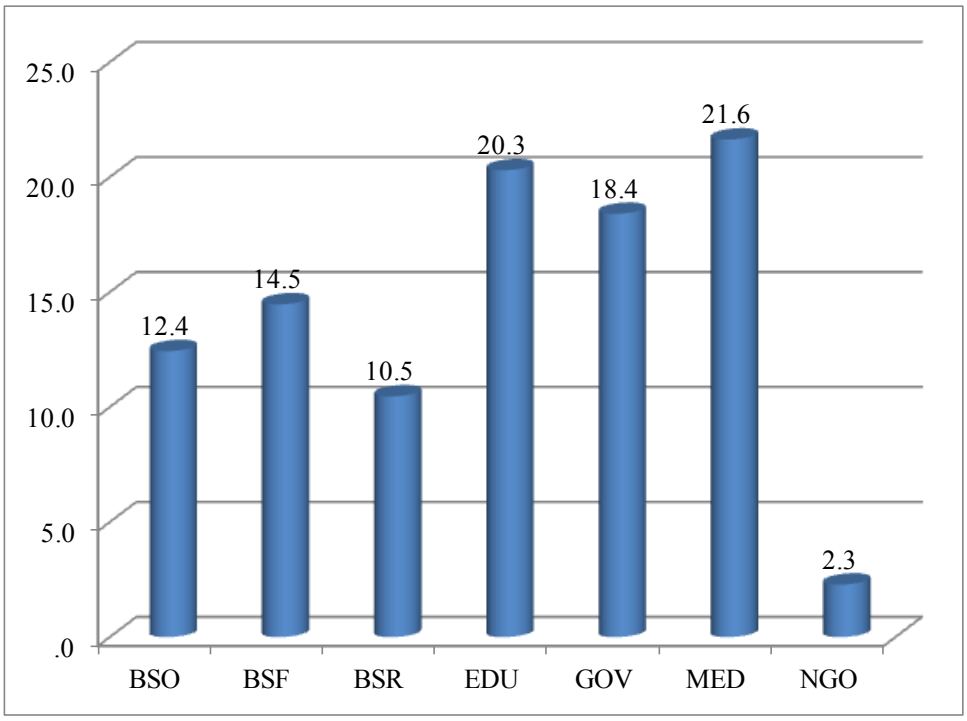


Figure 11 – Percent of Total Breach Frequency by Organization Type

As was done in Hypothesis 2, the findings in Figure 11 are evaluated further through computation of a Chi-squared statistic. Table 10 confirms that there is a statistically significant difference in the dispersion of breaches among organization types from the expected distribution based on random chance. It should be noted that Table 9 was calculated using the total number of breaches of each type and Table 10 was calculated using the total number of organizations within each type group. Figures 10 and 11 were displayed with the percentages instead of the raw numbers for clarity of presentation purposes only.

Test Statistics

	ORG_TYP
Chi-Square	536.714[a]
df	6
Asymp. Sig.	.000

a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 406.7.

Table 10 – Significance Test of Total Breach Frequency by Organization Type

Hypotheses 1 through 3 confirm that significant relationships do exist for breaches by breach type, organization type, and over time. A natural extension of this line of investigation is to wonder if a relationship between breach type and organization type may exist and, if significant, could it be exploited to the benefit of those parties involved in the assurance of, and/or consumption of, third-party service provider services. Due to the potential importance of this query, research question two will be devoted entirely to the investigation of breach type by organization type. Tables containing the supporting data for Figures 10 and 11 are provided in Appendix 7.

Research Question Two

Research question two is designed to specifically identify the breach type/organization type pairings that occur at a higher frequency level than expected. This is assuming that a significant and measurable relationship does exist between the two variables. Testing for Hypothesis 4 begins by employing measures to empirically establish or refute the existence of such a relationship. Note that Tables 37 through 43, containing supporting data for Figures 12 through 18 that address Hypothesis 4, are provided in Appendix 8 for those interested in the raw data.

While there is no universally-agreed rule as to the ranking of the strength of associations, many authors use the following general rule:

- -1.0 to -0.7 strong negative association
- -0.7 to -0.3 weak negative association
- -0.3 to +0.3 little or no association
- +0.3 to +0.7 weak positive association
- +0.7 to +1.0 strong positive association

Table 11 indicates that a statistically significant relationship exists between the breach type and the organization type variables in the data contained in the Privacy Rights Clearinghouse database. The non-parametric *phi coefficient* variant of the Chi-square correlation statistic is again evaluated from the table, as it is most appropriate when both variables are categorical (Nominal by Nominal). When evaluated based on this classification scheme, the association between BRCH_TYP and ORG_TYP is established as a weak positive association (Phi = .464) and it is statistically significant (Sig. = .000 at the .05 level).

Chi-Square

		Value	Asymp. Std. Error[a]	Approx. T[b]	Approx. Sig.
Nominal by Nominal	**Phi**	**.464**			**.000**
	Cramer's V	.189			.000
Interval by Interval	Pearson's R	.102	.018	5.492	.000[c]
Ordinal by Ordinal	Spearman Correlation	.109	.018	5.824	.000[c]
N of Valid Cases		2,847			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Based on normal approximation.

Table 11 - Association between Breach Type and Org Type

Having established that a statistically significant relationship does indeed exist between breach type and organization type, the next step is to further analyze individual components of that relationship in an attempt to identify specifics that may be exploited. To that end, the figures and tables on the following pages will analyze each organization type against all breach types so that specific guidance can be developed based on the threats most likely to be experienced by each organization type.

Figure 12 provides important information for auditors engaged by companies that fall into the Business-Other (BSO) organization type category, as it indicates that over 55% of all breaches suffered by these type entities are the result of only two breach types (Hacking or Malware, and Portable Device). Auditors of BSO organizations may be able to gain efficiencies by focusing their efforts in these two breach areas.

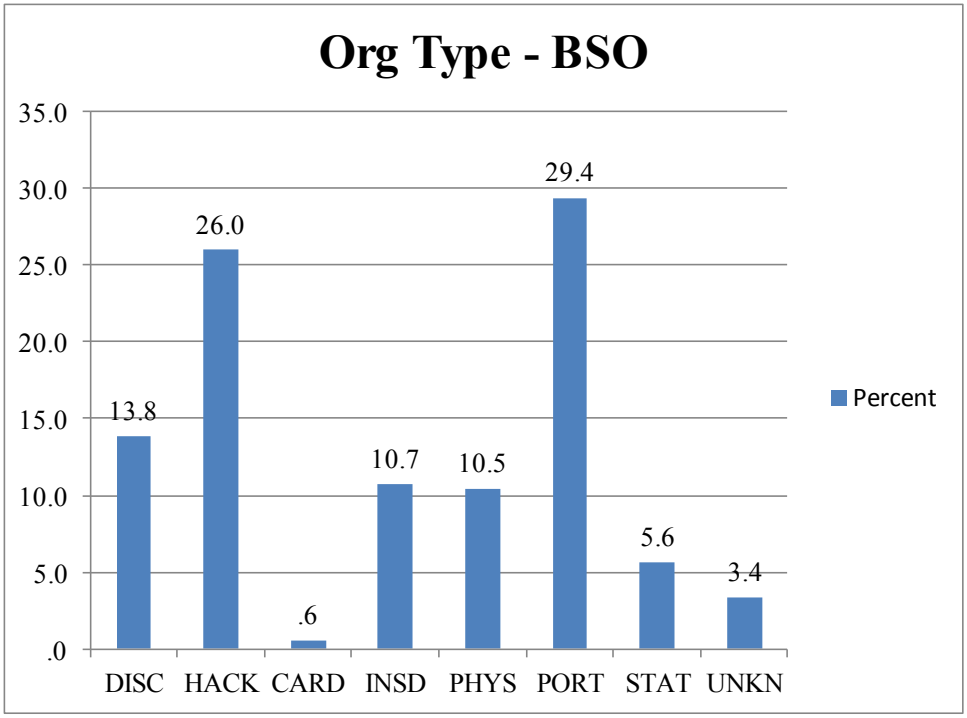


Figure 12 - Breaches for "Business-Other" Sector Entities (n = 354)

The significance of these findings are presented in Table 12, which indicates a significant positive association (*phi coefficient* = .084, p = .006).

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	19.927	7	.006
Likelihood Ratio	19.840	7	.006
Linear-by-Linear Association	.131	1	.717
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx.
Nominal by Nominal	**Phi**	**.084**	**.006**
	Cramer's V	.084	.006
N of Valid Cases		2,847	

Table 12 - Significance Test for "Business-Other" Sector

Figure 13 should prove useful to auditors engaged by companies that fall into the organization type Business, Financial and Insurance (BSF) category, since it indicates that over 60% of all breaches suffered by these type entities are the result of only three breach types (Hacking or Malware, Insider, and Portable Device). The Portable Device breach type alone accounts for over 30% of all breaches experienced by these type entities.

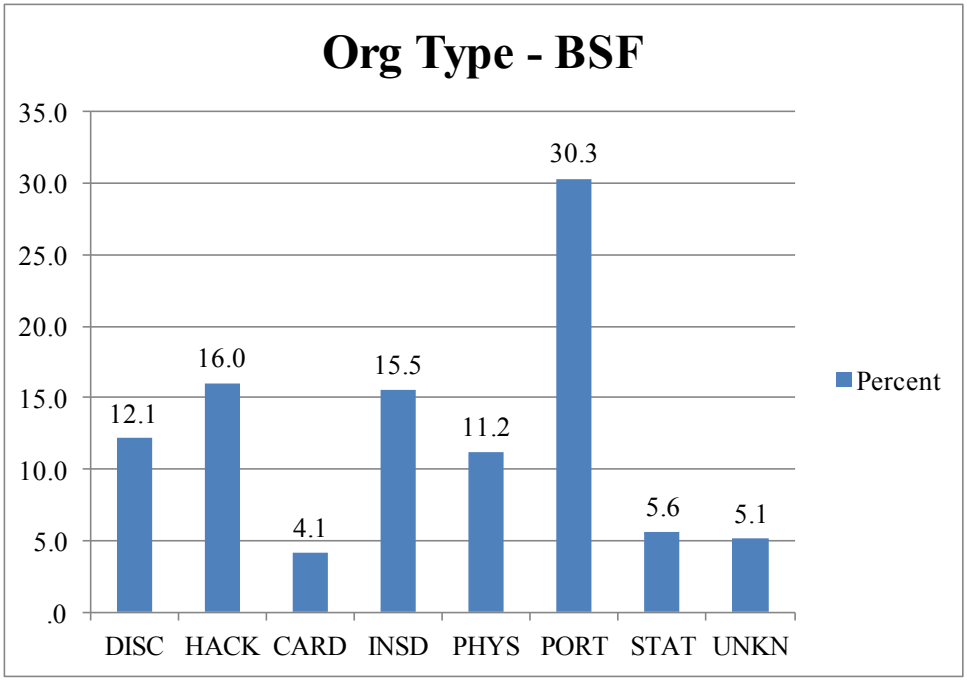


Figure 13 - Breaches for Business, Financial and Insurance Sector Entities (n = 412)

Confirmation of the significance of this relationship is provided in Table 13. The relationship is clearly significant (*phi coefficient* = .136, p = .000).

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	52.827	7	.000
Likelihood Ratio	45.582	7	.000
Linear-by-Linear Association	7.389	1	.007
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.136**	**.000**
	Cramer's V	.136	.000
N of Valid Cases		2,847	

Table 13 - Significance Test for Business, Financial and Insurance Sector Entities

Figure 14 provides similar data on organization type Business-Retail (BSR). Apparently, retail organizations are heavily targeted by hackers, as 36.6% of all retail breaches are associated with this source. Armed with this knowledge, auditors of these type entities would likely want to increase their examination of the internal controls designed to secure the entity's data assets from unauthorized access by external parties. They should work with systems designers to implement controls to detect and prevent such access from occurring before the external party has a chance to do any damage, or to at least minimize the damage that could be done.

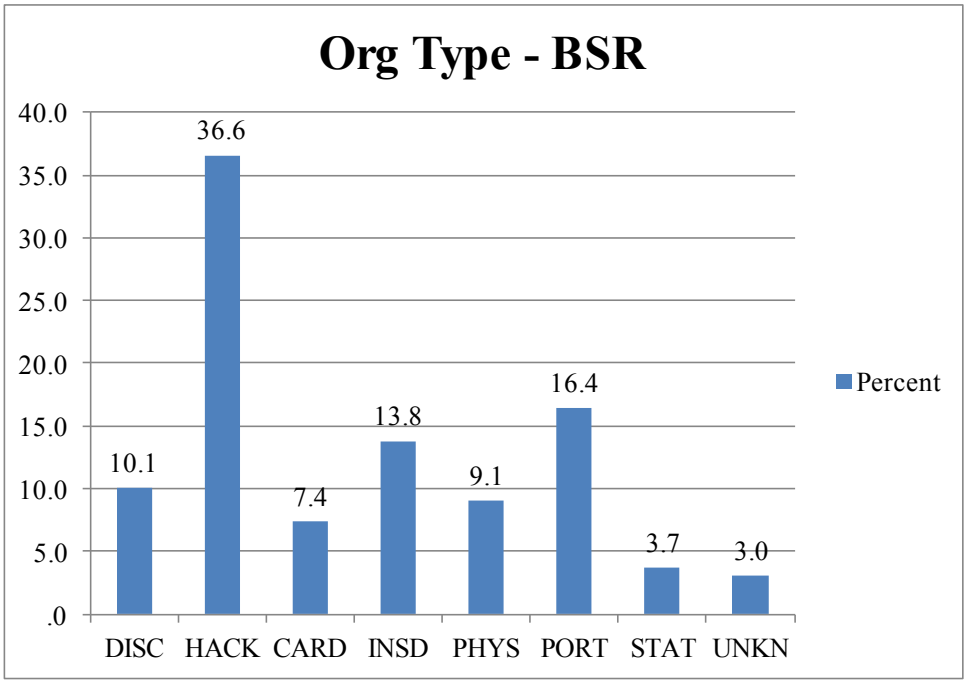


Figure 14 - Breaches for Retail Sector Entities (n = 298)

This relationship is indeed statistically significant as verified by the Chi-square statistics reported in Table 14 (*phi coefficient* = .249, p = .000).

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	176.035	7	.000
Likelihood Ratio	135.978	7	.000
Linear-by-Linear Association	21.565	1	.000
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.249**	**.000**
	Cramer's V	.249	.000
N of Valid Cases		2,847	

Table 14 - Significance Test for Retail Business Sector

Figure 15 provides results of the same analysis for educational institutions. As nearly 80% of all breaches occur in the top three breach categories (DISK, HACK & PORT), auditors could certainly benefit from this knowledge when working with clients in the EDU category. Working in conjunction with systems designers, auditors should be able to make great progress in preventing, or at least minimizing the impact of data breaches at Educational Institutions. Fully four-sevenths of the breach types could be ignored completely and the data indicates that Educational Institutions would benefit by a 79.4% reduction in breach exposure. Assuming that audit efforts are already being expended, it is likely that additional efforts would be unnecessary – all that is needed is to focus the current effort to gain the maximum benefit.

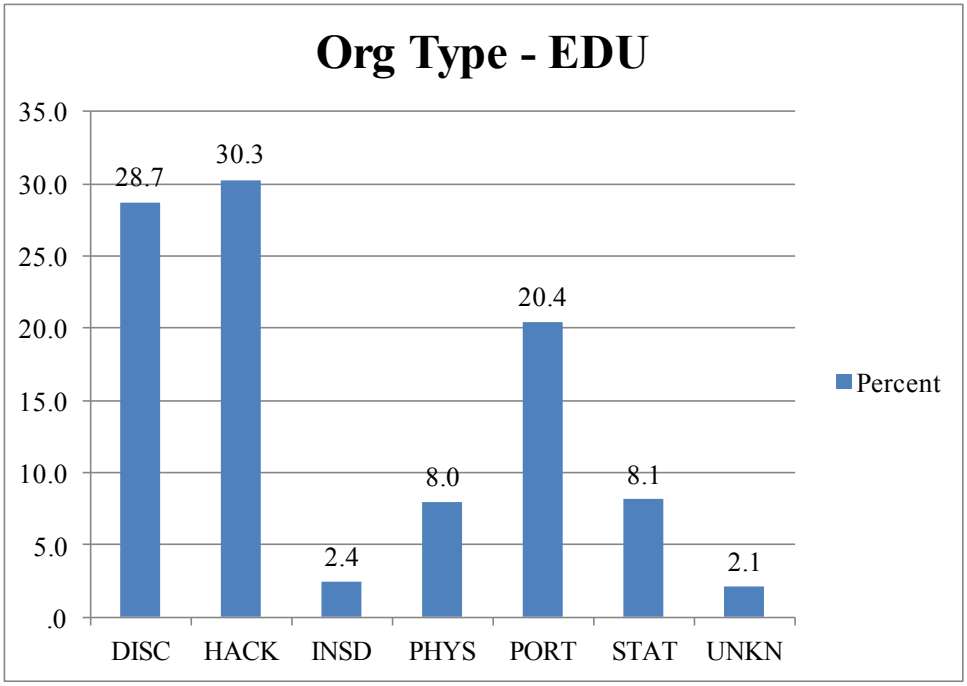


Figure 15 - Breaches for Educational Sector Entities (n = 578)

As in previous examinations, the Chi-square statistic is calculated and used here to confirm the significance of the relationship suggested in Figure 15. Significance is confirmed in Table 15 (*phi coefficient* = .261, p = .000).

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	194.446	7	.000
Likelihood Ratio	212.005	7	.000
Linear-by-Linear Association	86.261	1	.000
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.261**	**.000**
	Cramer's V	.261	.000
N of Valid Cases		2,847	

Table 15 - Significance Test for Education Sector

Governmental organizations appear to get hit hard on numerous fronts, as noted in Figure 16. However, since almost 55% of all breaches are classified into only two categories (DISC & PORT), this still represents an opportunity for auditors to streamline their approach to such an audit. The data indicates that almost three-fourths of breaches within a Government/Military type organization could be addressed by focusing all breach-related audit resources on only the Portable Device, Unintended Disclosure, and Physical Loss breach types. Some individuals may find certain breach type/organization type pairings curious. For example, why would Government/Military organizations be left alone by those responsible for the Hackers or Malware breach type, as is suggested by the data? Perhaps rather than signifying that they are not subjected to this type of breach, the data could be indicating that the Government/Military organizations are expending more of their resources in prevention of these breaches, and therefore their reported frequency is significantly lower. If this is the case, the data also indicate that these organization types are particularly sensitive to physical security, as evidenced by the Stationary Device breach category accounting for a mere 4% of the total breaches reported. This explanation is plausible, as it is widely known that governmental and military agencies are particularly attuned to physical security of property and physical access to locations and assets. The Educational Institutions organization type offers similarly interesting observations. Most prudent observers would probably agree that the security of the data that educational institutions possess is not nearly as critical as that of Government/Military organizations. Consequently, Educational Institutions organizations experience a significantly higher incidence of Hacking or Malware type breach. This could indicate that few resources are expended in these type organizations to combat breaches of this nature, as the cost/benefit to combat them is not justifiable.

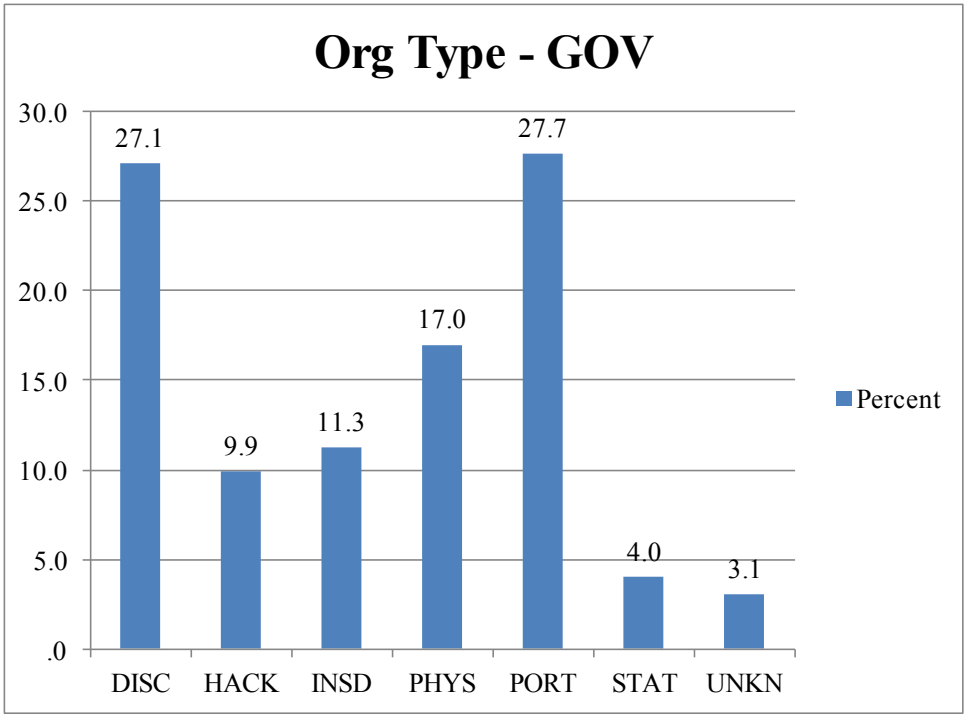


Figure 16 - Breaches for Governmental Sector Entities (n = 524)

The relationship is significant, as evidenced in Table 16 (*phi coefficient* = .171, *p* = .000).

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	82.795	7	.000
Likelihood Ratio	91.616	7	.000
Linear-by-Linear Association	2.729	1	.099
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.171**	**.000**
	Cramer's V	.171	.000
N of Valid Cases		2,847	

Table 16 - Significance Test for Governmental Sector

In medical organizations, almost 40% of all breaches experienced are traceable to just one breach type (PORT). This result is clearly significant, as evidenced by the statistics reported in Table 17. How best to address this issue is beyond the scope of the current research, but it clearly represents an opportunity for auditors to focus their examination in this area when auditing hospitals and other organizations classified in the MED category. Figure 17 implies the magnitude of this observation. Closer examination of this data also reveals that the percentage of reported breaches attributable to Hacking or Malware is significantly low, at only 4.5%. A very plausible explanation for this might be the high level of importance placed on prevention of data breaches as legislated by the HIPAA act of 1996. Under the provisions of this act, imposition of substantial fines and penalties were mandated for any business that allowed personal and/or medical data of patients to be accessed by unauthorized parties. It would appear that these type organizations have already been motivated to focus their resources toward prevention of breaches of this type.

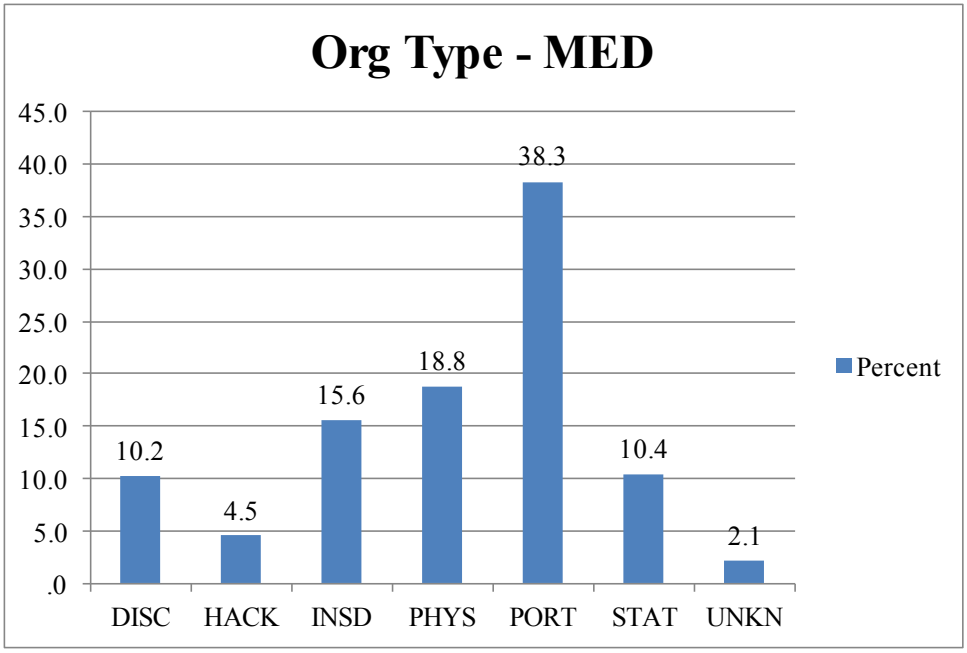


Figure 17 - Breaches for Medical Sector Entities (n = 616)

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	202.139	7	.000
Likelihood Ratio	235.996	7	.000
Linear-by-Linear Association	122.913	1	.000
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.266**	**.000**
	Cramer's V	.266	.000
N of Valid Cases		2,847	

Table 17 - Significance Test for Medical Sector

Following the pattern of the medical organizations, non-profit organizations also seem to suffer an unusually high incidence of breaches in the PORT category. As Figure 18 displays, this

single category accounts for over 43% of all breaches suffered by organizations classified as NGO. Most prudent individuals would deem this knowledge to be a clear opportunity to improve this statistic.

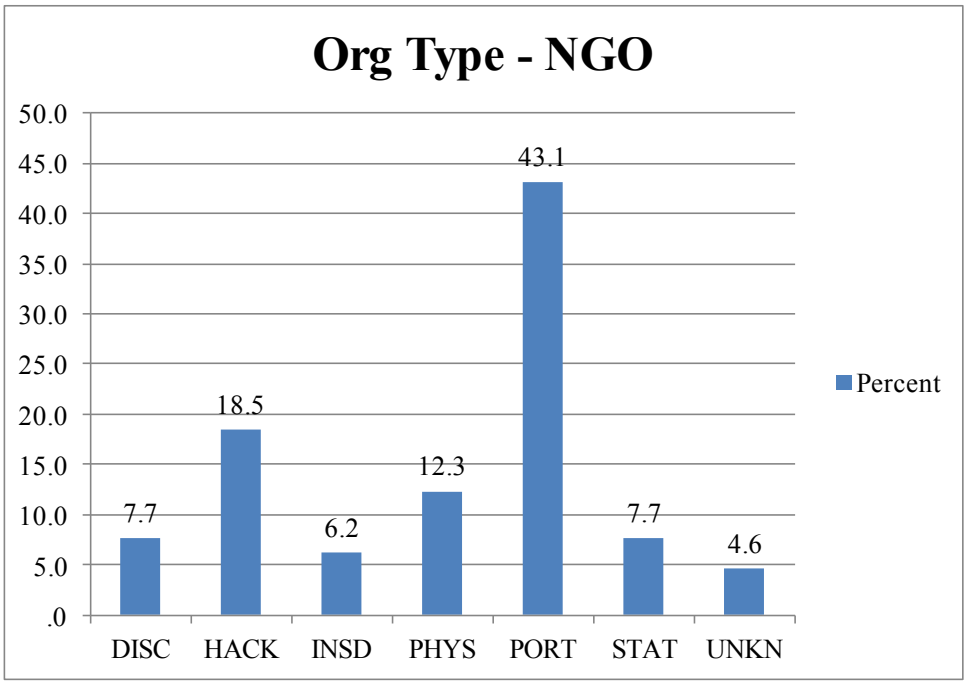


Figure 18 - Breaches for Non-profit Sector Entities (n = 65)

However, the result in the case of non-profit organizations differs from all the previous "breach type by organization type" analyses presented thus far, in that the result is not statistically significant. This is somewhat surprising because it certainly appears in Figure 18 that it would be significant. However, it is not, as is determined by the Chi-square test results presented in Table 18 (*phi coefficient* = .065, p = .099).

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	12.043	7	.099
Likelihood Ratio	13.481	7	.061
Linear-by-Linear Association	7.022	1	.008
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.065**	**.099**
	Cramer's V	.065	.099
N of Valid Cases		2,847	

Table 18 - Significance Test for Non-profit Sector

In the final analysis, all organization types exhibit strong associations with specific breach types, with the exception of the non-profit organization type. Armed with this knowledge, auditors may find that they can wring further efficiencies out of their audit engagements. However, developing audit guidelines is a lengthy and expensive process. Because of this, it may be more practical to group some of these associations together based on similarities, which would further simplify the process of incorporating the current research into the auditor's toolbox. To accomplish this, the next step is to perform a cluster analysis.

A cluster analysis is designed to group items into "clusters" that share common characteristics. A cluster is a group of relatively homogeneous observations – i.e., the objects in each cluster are similar in nature. It also means that items in a cluster are dissimilar to items in other clusters. Performing this analysis should allow auditors to narrow their focus, yet not get so narrow as to exceed the cost/benefit of the exercise. So instead of developing separate planning for each of the seven organization types and each of the eight breach types, they can

just develop plans that address a relatively few clusters. The similarity of cases in the cluster should allow for similar processes to address the breach challenges faced by organizations represented by that cluster. The results of the cluster analysis are presented in tables 19 through 21, below.

Cluster Distribution

	N	% of Total
Cluster 1	839	29.5%
2	765	26.9%
3	788	27.7%
4	455	16.0%
Total	2,847	100.0%

Table 19 - Overall Cluster Distribution

As indicated in Table 19, a cluster analysis of the breach types vs. organization types results in the data being allocated into only four clusters. In the following discussion, since there are only 4 clusters, any contribution to a cluster of 25% or more is deemed to be an important contributor to that cluster and are bolded in Tables 20 and 21 to so indicate. The clusters were derived based on the following data groupings:

BRCH_TYP

	DISC		HACK		CARD		INSD		PHYS		PORT		STAT		UNKN	
	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%
Cluster 1	437	**86.5%**	402	**75.3%**	0	.0%	0	.0%	0	.0%	0	.0%	0	.0%	0	.0%
2	63	12.5%	0	.0%	2	4.9%	207	**65.5%**	288	**78.0%**	0	.0%	152	**79.6%**	53	**61.6%**
3	5	1.0%	132	**24.7%**	0	.0%	4	1.3%	8	2.2%	631	**78.4%**	5	2.6%	3	3.5%
4	0	.0%	0	.0%	39	**95.1%**	105	**33.2%**	73	19.8%	174	21.6%	34	17.8%	30	**34.9%**
Total	505	100%	534	100%	41	100%	316	100%	369	100%	805	100%	191	100%	86	100%

Table 20 - Clusters based on Breach Type

Table 20 defines which breach types are most closely identified by each cluster. For example, Cluster 1 contains only DISC and HACK type breaches. Cluster 2 is predominantly comprised of INSD, PHYS, STAT, and UNKN breaches. Cluster 3 is almost entirely PORT and HACK, and Cluster 4 is mainly CARD, INSD and UNKN. A similar breakdown of the information by organization type is presented in Table 21 below.

ORG_TYP

	BSO		BSF		BSR		EDU		GOV		MED		NGO	
	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%
Cluster 1	49	13.8%	116	**28.2%**	139	**46.6%**	341	**59.0%**	194	**37.0%**	0	.0%	0	.0%
2	109	**30.8%**	0	.0%	0	.0%	119	20.6%	185	**35.3%**	352	**57.1%**	0	.0%
3	196	**55.4%**	0	.0%	0	.0%	118	20.4%	145	**27.7%**	264	**42.9%**	65	**100%**
4	0	.0%	296	**71.8%**	159	**53.4%**	0	.0%	0	.0%	0	.0%	0	.0%
Total	354	100%	412	100%	298	100%	578	100%	524	100%	616	100%	65	100%

Table 21 - Clusters based on Organization Type

As indicated, Table 21 defines which organization types are most closely identified by each cluster. So Cluster 1 is comprised of BSF, BSR, EDU and GOV organization types. Cluster 2 is predominantly BSO, GOV, and MED. Cluster 3 is largely populated by BSO, GOV and MED organizations, and Cluster 4 is almost entirely BSF and BSR. Crossing the information from Tables 20 and 21 allows the development of a description of a representative of each cluster, and therefore will enhance audit focus because simply identifying the cluster membership of the client organization, auditors can concentrate on the breaches most likely to occur to organizations within that cluster. For example, Cluster 1 is predominantly comprised of organization types BSF, BSR, EDU and GOV, and almost entirely breach types DISC and HACK. Therefore, if the client organization is BSF, BSR, EDU or GOV, the auditor's resources in regards to breaches should be concentrated on detecting and/or preventing DISC and HACK

type breaches. A similar descriptive breakout of breach/organization type correlation (group membership description) can easily be determined for clusters 2, 3 and 4. Note that while relying on the cluster analysis may reduce workload somewhat for auditors, some granularity is lost by combining the cases together in this manner. This could result in less effective procedures being applied in some audits.

Research Question Three

Research question three seeks to answer multiple questions, namely: a) if prior breach experience has any effect on the current outsourcing decision, b) if certification level impacts the current outsourcing decision, and c) if personal knowledge of assurance levels impacts the current outsourcing decision. In this portion of the study, the issues under examination are of a different nature. Consequently, the testing methods employed will differ from those used in the previous section.

Testing for Hypothesis 5a is designed to establish if prior breach exposure has an impact on an IT director's future outsourcing decisions. The testing was designed to examine the relationship between the PRIOR_BRCH variable (which is based on the "yes" responses to either of questions 4a or 4b of the survey) with the future INTENT variable (derived from question 5 of the survey). Unfortunately, as indicated by the absence of any valid "yes" responses (i.e. "1s") in table 22 below, not a single survey was returned that claimed any experience with prior breaches.

Survey Question 4a

		Frequency	Percent	Valid Percent
Valid	0	97	47.8	100.0
Missing	System	106	52.2	
Total		203	100.0	

Survey Question 4b

		Frequency	Percent	Valid Percent
Valid	0	97	47.8	100.0
Missing	System	106	52.2	
Total		203	100.0	

Table 22 - Frequency Data for Survey Questions 4a & 4b

This could be interpreted to mean that breaches are just not as prevalent as originally believed, but it is much more likely to indicate selection bias – i.e., those that have previously experienced breaches may have opted not to participate in the survey for this or some other reason. Unfortunately, lack of any positive responses to questions 4a and 4b makes statistical evaluation of Hypothesis 5a impossible. Due to this complication, no inferences whatsoever should be made based on this data.

As is the case with Hypothesis 5a, evaluation of Hypothesis 5b is dependent upon having a testable population of responses to questions 4a and 4b. The intent of Hypothesis 5b was to isolate the audited versus unaudited component of the INTENT variable and look for an effect of the audit experience on the future intent of IT directors. Due to the limitations imposed by the small and possibly biased sample response pool, Hypothesis 5b is also un-testable.

Hypothesis 6 is designed to examine the level of confidence that IT decision-makers have in the assurance given by audit reports issued on third-party service providers, and the role it plays on their future outsourcing decisions. Testing of this relationship requires a comparison of the INTENT variable with the AUDIT_IMPT variable. As indicated by the frequency analysis in Table 23, of the 203 respondents to the survey, only 14 even answered the INTENT question (6 positive and 8 negative responses).

Survey Question 5 (INTENT)

		Frequency	Percent	Valid Percent
Valid	0	8	3.9	57.1
	1	6	3.0	42.9
	Total	14	6.9	100.0
Missing	System	189	93.1	
Total		203	100.0	

Table 23 - Future Outsourcing Intent

Table 24 presents the frequency analysis of the AUDIT_IMP variable. Of the 14 observations reported in Table 23 for question 5, only 11 also answered survey question 6. This leaves a sample so small that any test performed would lack sufficient power to be valid.

Survey Question 6 (AUDIT_IMP)

		Frequency	Percent	Valid Percent
Valid	1	25	12.3	**31.6**
	2	3	1.5	3.8
	3	5	2.5	6.3
	4	6	3.0	7.6
	5	7	3.4	8.9
	6	2	1.0	2.5
	7	7	3.4	8.9
	8	6	3.0	7.6
	9	18	8.9	**22.8**
	Total	79	38.9	100.0
Missing	System	124	61.1	
Total		203	100.0	

Table 24 - Importance of 3rd-Party Service Provider Audits

Taken together, Tables 23 and 24 provide only 11 observations on which to test Hypothesis 6. Clearly there is a lack of sufficient data to perform the planned binary logistic regression and make any meaningful evaluation of the result.

Finally, Hypothesis 7 seeks to determine if an IT director's level of understanding of the differences in assurance implied by the various auditor reports has an effect on his or her future outsourcing intent. This was to be accomplished by comparing the future intent variable (INTENT) with the familiarity variable (KNOW) via a simple binary logistic regression. However, as is evident in Table 23 above, a maximum of 14 observations would be possible in this analysis as this is the total responses to survey question 5 (INTENT). The analysis for Hypothesis 7 is further limited because only 12 of the 14 potential responses also contained a response to survey question 7 (KNOW). Consequently, no meaningful analysis can be performed on this data either.

In the examination of Hypotheses 6 and 7 above, the indicated tests were performed on the extremely limited sample(s) available. However, the results are not reported here due to the belief that no reliable inferences can be drawn from such limited data. The findings from these analyses are provided in Appendices 9 and 10 for those parties who may still want to view them. Extreme caution is warranted when evaluating these tables and any attempt to make inferences based on them is strongly discouraged. As shown in Table 25, of the 203 valid responses received, only question 7 contained a response from more than 50% of the respondents. Some were so low as to be effectively useless, like the 14 total valid responses to question 5.

Frequency

		SQ1	SQ3	SQ4a	SQ4b	SQ5	SQ6	SQ7
N	Valid	203	77	97	97	14	79	111
	Missing	0	126	106	106	189	124	92

Table 25 - Survey Response Frequency

As in the case for testing of hypotheses 5 through 7, adequate data was not available to run the calculation of the overall regression presented in association with Figure 2 of Chapter III.

The effort expended on this portion of the study was not, however, completely in vain. Some patterns emerge from an analysis of the responses from the survey that may prove interesting and provide impetus to future studies. For example, as indicated in Table 26, over 38% of all respondents indicate that they do in fact consider themselves to be consumers of cloud services in one form or another. This is a fairly high percentage, considering all the concerns associated with cloud usage.

Survey Question 1 (USE_CLOUD)

		Frequency	Percent	Valid Percent
Valid	0	125	61.6	61.6
	1	78	38.4	**38.4**
	Total	203	100.0	100.0

Table 26 - Cloud Use

Another observation that may be of interest is illuminated in Table 27. Of the 203 total responses, only 77 even knew whether or not their 3rd-party service provider had audit services performed, which represents only 38%. An even smaller number (27) indicated that the audits were in place. This indicates that barely 13% of the entities that are consuming cloud services can confirm that their 3rd-party service provider has benefit of audit services of some type.

Survey Question 3 (CSP_AUDITED)

		Frequency	Percent	Valid Percent
Valid	0	50	24.6	64.9
	1	27	**13.3**	35.1
	Total	77	**37.9**	100.0
Missing	System	126	62.1	
Total		203	100.0	

Table 27 - 3rd-party Service Provider Audited?

It appears that consumers of cloud services are either not aware of the assurance services provided by the accounting profession regarding 3rd-party service providers, or they simply don't see the value in such services and consequently consume without regard for security assurance in any form.

An examination of Table 28 reveals that responders seem to be polarized on the importance of assurance service reporting on their 3rd-party service providers, with 31.6% placing minimal importance on the reporting and 22.8% indicating that it is critical.

Survey Question 6 (AUDIT_IMP)

		Frequency	Percent	Valid Percent
Valid	1	25	12.3	**31.6**
	2	3	1.5	3.8
	3	5	2.5	6.3
	4	6	3.0	7.6
	5	7	3.4	8.9
	6	2	1.0	2.5
	7	7	3.4	8.9
	8	6	3.0	7.6
	9	18	8.9	**22.8**
	Total	79	38.9	100.0
Missing	System	124	61.1	
Total		203	100.0	

Table 28 – Reported Importance of 3rd-party Service Provider Audit Reports

As reported previously in this study, only those engagements resulting in the issuance of an SOC type 2 or type 3 report are specifically designed to address issues associated with data security and integrity in the audit of a 3rd-party service provider. Survey question seven was specifically constructed to determine if this information is known to the consumers of cloud services. It appears that the accounting profession is failing in its efforts to enhance the perceived value of this service by educating the potential consumer market. As evidenced in Table 29, only 16.2% of respondents who answered this question claimed to know the difference in the audit reports issued on 3rd-party service providers. This means that 83.8% would potentially consume cloud services blindly, or they believe themselves to be afforded some sort

of protection (by relying on the incorrect reports) that simply is not there. This improper use of the reports and lack of understanding is one of the primary reasons that SAS70 was retired in the first place, yet it would appear that the "new and improved" version is not working any better. It is probably fair to assume that the numbers would not get better if the response rate on this question was higher, as some responders likely left it blank rather than admit to a lack of knowledge that they probably should possess, given their positions within their organizations.

Survey Question 7 (KNOW)

		Frequency	Percent	Valid Percent
Valid	0	93	45.8	83.8
	1	18	8.9	**16.2**
	Total	111	54.7	100.0
Missing	System	92	45.3	
Total		203	100.0	

Table 29 - Knowledge of 3rd-party Service Provider Reporting

While the above observations were not the initial focus of this portion of the study, they do nevertheless help salvage something of value from the effort expended.

Chapter V

CONCLUSIONS

The primary goals of this study were: to identify anomalies in reported breach data that could be exploited to the benefit of auditors, and to empirically establish that reported breach frequency varies significantly between various pairings of breach type and organization type. This information could greatly assist auditors in the risk assessment portion of their engagement planning, as the engagement resources can be focused on addressing those breach events more likely to occur, based on the type of organization under review. An additional objective is to identify factors that affect the decisions of CIOs regarding their consideration of whether to employ cloud/datacenter-hosted solutions and examine their level of awareness regarding the different assurance levels offered by these various third-party service provider audit reports. Ultimately, the research sought to answer these questions:

1. Are there any significant anomalies in reported breach data that could be used to benefit auditors?
2. If type of organization is significantly associated with type of breach, which organization types are most vulnerable to which types of breaches?

3. Do any of the following influence CIOs when making outsourcing (cloud) decisions?

   Prior breach experience
   Level of importance placed on audit certification
   Level of personal knowledge of assurance levels

The research has shown that anomalies definitely do exist that could prove useful to auditors and systems designers. Looking strictly at types of breaches, three of the eight breach types (DISK, HACK & PORT) comprise 65% of the total breaches reported. Consequently, lacking any other information upon which to base their decision, auditors should apply an appropriate percentage of their breach detection and/or prevention resources to these three breach types. The analysis strictly by organization type was equally enlightening, indicating that three of the seven (EDU, GOV & MED) organization types account for over 60% of total reported breaches. Again, sans better information, auditors should expend a larger percentage of their resources in the detection and/or prevention of breaches when auditing organizations that fit into one of these three categories. One caveat that should be considered here is that many entities included in organization types EDU, GOV and MED are also non-profit entities. In the overall analysis of breaches by organization type, nonprofit organizations (NGO) accounted for only 2.4% of the total breaches. However, considering that a large portion of EDU, GOV and MED entities are also NGO entities, the data would indicate that nonprofit organizations report roughly two-thirds of all breaches reported. It is quite possible that this is indicative of an underlying unrelated factor, such as: perhaps for-profit entities are underreporting their breaches, or perhaps they have better controls. Either way, there are very clear trends in breaches noted over the study period.

A statistically significant relationship was established between the type of breach and the type of organization reporting those breaches. This information could prove quite useful to

auditors when planning and conducting their examinations. Unfortunately, there were no factors identified that influence the decisions of IT directors regarding the consumption of distributed network/cloud services. This was not due to failure to find statistical significance, but rather is a remnant of such a poor survey response as to render this part of the study un-testable. There were, however, a number of observations made from the frequency analysis of the small data sample that may indicate areas ripe for future research.

It is important to keep an open mind when considering a foray into the cloud computing environment, and maintaining a healthy skepticism will likely serve any CIO well. The marketing hype that extols the virtues of the cloud and all its possibilities is to be expected. However, this spin has been enjoined by the mainstream media to the point that anti-cloud sentiment is not nearly as widely published or available. Much of this research project has elucidated that there are still serious concerns with the cloud – particularly in the area of security. However, CIOs should also recognize that some of the most important promises of the cloud may not materialize. Cost savings, for example, is one of the most widely touted reasons for outsourcing services into the cloud. Most of the articles written on the subject make a claim of some sort based on cost savings. Yet very recent reports warn users that this just simply is not always true because the implementation and operation of cloud services can become extremely complex and pricing models can be extremely convoluted. An article in the March 6, 2012 journal *CFO* explains how an Australian company considering replacing an aging enterprise system came to the conclusion that a SaaS solution would cost between 135% and 280% more than purchasing an on-premises replacement system, due to the added complexities and the unanticipated "per transaction" costs that the SaaS contract included. The author warns readers to: "Just make sure that when you launch your own cloud initiative, the driver is not enthusiasm

for the technology but a deep knowledge of your own business requirements" (Livingstone, 2012).

For any readers who still doubt the dangers lurking in the cloud for the unwary, the following example may sway their position. The *Washington Post* reported on April 2, 2012 on a security breach that may have compromised millions of debit and credit cards. The article states that Mastercard and Visa were trying to determine the extent of a breach at an Atlanta-based payment processing company that describes itself as "one of the world's largest electronic transaction processing companies." In the cloud, as in real estate, caveat emptor is the rule, not the exception.

Contributions of the Research

This research identified factors common to data breaches and the organizations that report them. As such, it provides opportunities for auditors to focus their examination of data breaches performed in an audit, based on the organization type. This allows critical resources to be deployed where they are statistically most likely to be effective in preventing and/or detecting data breaches. Numerous parties will benefit from this research, namely: 1) CPA firms that provide security-related attest services to third-party service provider organizations, as they will have opportunities to plan and conduct their audits more efficiently and effectively, 2) third-party service provider companies (those that consume SAS70/SSAE16/SOC audit services), as they may see a reduction in their breach frequency, thereby enhancing their image and the value of their services; their audits may also be more efficient and therefore less costly, 3) CPA firms that audit cloud consumer organizations, because their external auditors can place more reliance on the work of the service organization auditor, and finally, 4) the cloud services consumer

organizations, as they may experience lower audit fees through efficiencies recognized in 3) above. All of this may also promote enhanced trust in cloud systems and therefore, growth of the industry. The ultimate contribution of this research is that it provides additional tools to regulators and auditors, which they can use in the fight against the ever-growing problems associated with data breaches – i.e., identity theft, financial fraud, etc.

Armed with the findings from this study, auditors can better focus their efforts. For example, when auditing a nonprofit organization, much greater emphasis should be placed on confirmation of proper procedures and controls related to laptops and other portable devices. This single breach type accounts for: more than 20% of reported breaches for educational institutions, almost 28% for Government/Military organizations, fully 38.3 % for Medical organizations, and 43.1% for entities classified in the nonprofit category. Clearly, auditors need to more closely examine the policies and procedures related to laptops and portable devices, and perhaps even address the proper education of personnel as to those policies and procedures and their importance to the organization.

Governmental agencies and educational institutions also stand to gain considerably from this research, as they too are frequent victims of data breaches and suffer the associated economic penalties.

Another contribution of this research is in the impact it may have on the cloud services industry as a whole. Identification of factors that influence the decisions of IT directors is the first step in addressing their concerns. While the current project was unable to definitively identify such factors, the frequency analyses of the survey data did provide some interesting observations that will guide future research in this area. Once relevant factors are specifically identified, future assurance services can be targeted toward addressing the associated concerns,

thereby enhancing the growth of the cloud services industry overall. Finally, the conceptual model that was developed will be useful in future research designed to isolate and quantify those factors that influence IT directors in their decisions to consume cloud-related services.

Future Research

Both cloud services and data breaches are areas with great potential for future research. This is true not only because of the recent popularity of these areas, but also due to their large growth projections. This study suggests several avenues of future research that might prove interesting. One observation from the data is that the trend in breaches was steadily downward from 2006-2009, then turned upward. Further analysis in this area might reveal causal factors for this phenomenon. The ability to identify factors that drive breach frequency would be quite valuable in the development of tools to help combat the problem. Another area of investigation that might prove interesting is the relationship between the number of records breached and the number of breaches. Does the loss potential associated with a breach truly depend on the number of records breached, as current thinking suggests, or are there other factors that play a more important role? Perhaps some other factors that could be more easily manipulated, and therefore provide greater opportunities for minimizing the economic effect of breaches that occur? Since this study identifies trends over time based on breach type, it might prove useful to also examine the impact of well-known malware outbreaks and other such widespread web-based attacks on the observed trends. The current study identified factors that account for some of the variability in reported breaches. Future studies of a more predictive nature may contribute greatly to the knowledge in this area, while also aiding in efforts to control the problem.

The survey portion of this study attempted to address important questions that need to be answered in order to enhance the data security provided by 3rd-party service providers. While the survey results did not provide specific guidance, these questions still need to be answered, and there were still some good observations. Future studies should attempt to answer the questions posed in this section perhaps through other means. In the "remarks" section of the survey, numerous respondents expressed that in their opinion, SurveyMonkey™ or a similar survey tool would be a much better methodology for conducting a survey of this nature. Some went to the trouble to respond just to offer this suggestion, without bothering to participate in the study by completing the survey. A future study might replicate the current study using such a tool and perhaps would enjoy a much improved response rate. Other data that was included in the survey email list that was purchased, such as industry type might also prove useful in future research. A comparison of the breach data from the first section of the current study with the responses by NAICS code might provide some clues as to why some of the trends in breaches by type and industry exist.

Bibliography

References

AICPA. (2010, May 9). SAS No. 70 and Service Organizations. Retrieved October 14, 2011, from AICPA: http://www.aicpa.org/_catalogs/masterpage/Search.aspx?S=SAS+70+guidance

AICPA. (2012). Trust Services. Retrieved Jan 17, 2012, from American Institute of CPAs: http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/TRUSTSERVICES/Pages/default.aspx

AICPA. Auditing Standards Board. (1984, July). Effects of computer processing on the examination of financial statements. Retrieved April 4, 2012, from University of Mississippi Library. Accounting Collection: http://umiss.lib.olemiss.edu:82/record=b1038071

AICPA. Auditing Standards Board. (1982, December). Special-purpose reports on internal accounting control at service organizations. Retrieved April 4, 2012, from University of Mississippi Library. Accounting Collection: http://umiss.lib.olemiss.edu:82/record=b1038066

AICPA. Auditing Standards Executive Committee. (1974, December). Effects of EDP on the auditor's study and evaluation of internal control. Retrieved April 4, 2012, from University of Mississippi Library. Accounting Collection: http://umiss.lib.olemiss.edu:82/record=b1038020

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., et al. (2009). Above the Clouds: A Berkeley View of Cloud Computing. Berkeley: University of California at Berkeley.

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011, May 12). NIST Computer Security Resource Center - Publications - SP800-146.pdf. Retrieved October 2, 2011, from NIST Information Technology Laboratory: http://csrc.nist.gov/publications/PubsDrafts.html

Baker, W., Hutton, A., Hylender, C. D., Pamula, J., Porter, C., & Spitler, M. (2011). 2011 Data Breach Investigations Report. Arlington: Verizon RISK Team.

Baskerville, R., & Siponen, M. T. (2002). An information security meta-policy for emergent organizations. Logistic Information Management , 15, 337-346.

Bell III, T. J. (2010). Integrating IT Auditing (SAS 70 Reporting) to Benefit both the User and Service Organizations: An Organizational Change Perspective. Proceedings of the Decision Sciences Institute - Southwest Region (pp. 1-17). Dallas: SWDSI.

Berg, N. (2005). Non-Response Bias. In K. E. Kempf-Leonard, ENCYCLOPEDIA OF SOCIAL MEASUREMENT (Vol. 2, pp. 865-873). London: Academic Press.

Brenner, B. (2010, October 6). Data Protection. Retrieved September 22, 2011, from CSO Security and Risk: http://www.csoonline.com/article/622277/sas-70-replacement-ssae-16

Brunette, G., & Mogull, R. E. (2011). Cloud Security Alliance Home page. Retrieved September 22, 2011, from Cloud Security Alliance: https://cloudsecurityalliance.org/wp-content/uploads/2011/07/csaguide.v2.1.pdf

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security , 11, 431-448.

Chakraborty, R., Ramireddy, S., Raghu, T. S., & Rao, H. R. (2010). The Information Assurance Practices of Cloud Computing Vendors. IT Professional , 29-37.

Clegg, S., Hardy, C., & Nord, W. R. (1996). Handbook of Organization Studies. In J. Barney, & W. Hesterly, Organizational Economics: Understanding the Relationship between Organizations and Economic Analysis (pp. 115-147). London: Sage.

Cloud Security Alliance. (2009, December 15). CSA Security Guide V2.1. Retrieved August 30, 2011, from Cloud Security Alliance: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

Cloud Security Alliance. (2011). About CSA. Retrieved October 17, 2011, from Cloud Security Alliance: https://cloudsecurityalliance.org/about/

Committee on Auditing Procedure, American Institute of Accountants. (1939, May 9). Digital Collections: Deloitte Collection. Retrieved April 3, 2012, from University of Mississippi Libraries: http://clio.lib.olemiss.edu/cdm4/document.php?CISOROOT=/deloitte&CISOPTR=10100&CISOSHOW=10088

Committee on National Security Systems. (2010, April 26). CNSS Instructions. Retrieved September 29, 2011, from The Committee on National Security Systems: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

DataTrendsPublications. (2011, April 26). Data Trends Reports: Cloud Computing. Retrieved April 4, 2012, from Data Trends Publications: http://datatrendspublications.blogspot.com/2011/04/sixty-percent-of-companies-using.html

DeFelice, A., & Leon, J. F. (2010). Cloud Computing: What accountants need to know. Journal of Accountancy , 210 (4), 50-55.

Dennis, B. (2012, April 2). *Security breach may have compromised millions of debit and credit cards.* Retrieved April 5, 2012, from The Washington Post with Bloomberg Business: http://www.washingtonpost.com/business/economy/security-breach-may-have-compromised-millions-of-debit-and-credit-cards/2012/03/30/gIQAkUkAmS_story.html

Dhillon, G. (2004). Guest Editorial: The challenge of managing information security. International Journal of Information Managmenet , 24, 3-4.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal , 11, 127-153.

Dyer, J. H., & Singh, H. (1998). The Relational View: Cooperative Strategy and Sources of Interorganizational Competitive Advantage. The Academy of Management Review , 23 (4), 660-679.

Emerson, R. M. (1976). Social Exchange Theory. Annual Review of Sociology , 2, 335-362.

Feeny, D., Lacity, M., & Willcocks, L. (2005). Taking the measure of outsourcing providers. MIT Sloan Management Review , 46 (3), 41-48.

Finch, C., & Oricchio, R. (2011, July 28). Business Bytes. Retrieved August 28, 2011, from Inc.com: http://www.inc.com/tech-blog/from-sas-70-to-ssae-16-how-to-keep-your-cloud-service-on-track.html

Freedman, D. H. (2011, September 21). Small Business. Retrieved October 22, 2011, from The New York Times Business Day: http://www.nytimes.com/2011/09/22/business/smallbusiness/what-to-consider-when-thinking-about-moving-to-the-cloud.html?_r=1&adxnnl=1&adxnnlx=1319292043-SWVPiUr1VwuI5KuWu9iLaA

Gellman, R. (2011). Home Page. Retrieved October 20, 2011, from World Privacy Forum: http://www.worldprivacyforum.org/

Gens, F. (2009, Dec 15). IDC Exchange Blogs. Retrieved Jan 28, 2012, from IDC: http://blogs.idc.com/ie/?p=730

Gottschalk, P., & Solli-Sæther, H. (2005). Critical success factors from IT outsourcing theories: an empirical study. Industrial Management & Data Systems , 105 (6), 685-702.

Gottschalk, P., & Solli-Sæther, H. (2006). Maturity model for IT outsourcing relationships. Industrial Management & Data Systems , 106 (2), 200-212.

Graham, J. D. (2011, April). Navigating the Cloud: Insights and Guidance from Cloud Connect 2011. Retrieved February 2, 2012, from Grail Research: http://grailresearch.com/pdf/ContenPodsPdf/Grail-Research-Navigating-the-Cloud.pdf

Hancock, B. (1999). Online Fraud Increasing Rapidly. Computers adn Security , 18, 194.

Hechter, M. (2008). The rise and fall of normative control. Accounting, Organizations and Society , 33, 663-676.

Hickey, A. R. (2010, August 25). IaaS Isn't Just Cloud Computing Fluff: Survey. Retrieved April 4, 2012, from CRN.com: http://www.crn.com/news/cloud/227001081/iaas-isnt-just-cloud-computing-fluff-survey.htm;jsessionid=6yZ5LRHN5jvdRkGCo8wpTQ**.ecappj01

i365.com. (2010). cloud-storage-services. Retrieved July 23, 2011, from i365.com.: http://www.i365.com/products/cloud-storage-services/

ISAE3402.com. (2011). ISAE3402 Overview. Retrieved 9 18, 2011, from ISAE3402.com: http://isae3402.com/ISAE3402_overview.html

Julisch, K., & Hall, M. (2010). Security and Control in the Cloud. Information Security Journal: A Global Perspective , 19, 299-309.

Kadam, Y. (2011). Security Issues in Cloud Computing: A Transparent View. International Journal of Computer Science & Emerging Technologies , 2, 316-322.

Kaliski Jr., B. S., & Pauley, W. (2010). Toward Risk Assessment as a Service in Cloud Environments. HotCloud'10 Proceedings of the 2nd USENIX conference on Hot topics in cloud computing (p. 13). Boston: USENIX Association, Berkeley, CA, USA.

Kaliski, B., & Pauley, W. (2010). Toward Risk Assessment as a Service in Cloud Environments. Proceedings of the 2nd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud'10), (pp. 20-29). Boston.

Kuttikrishnan, D. (2011, August 2). Cloud Computing: The Road Ahead. Retrieved February 17, 2012, from Datamation: http://www.datamation.com/cloud-computing/cloud-computing-the-road-ahead-1.html

Leavitt, N. (2009). Is Cloud Computing Really Ready for Prime Time? Computer , 42, 15-20.

Livingstone, R. (2012). Choosing a Cloud Application: A Hornet's Nest of Complexity. *CFO*, 1-2.

Mark Bednarz, C. (2010, July). Wall Street Argus. Retrieved September 24, 2011, from Rothstein Kass: http://www.rkco.com/Corporate/Admin/AttachmentFiles/wall_street_argus/RK_WallStreetArgus_7_10_SSAE16.pdf

Nicolaou, C. A., Nicolaou, A. I., & Nicolaou, G. D. (2012). Auditing in the Cloud: Challenges and Opportunities. The CPA Journal , 82 (1), 66-70.

Open Cloud Manifesto. (2011). FAQ. Retrieved October 27, 2011, from Open Cloud Manifesto: http://www.opencloudmanifesto.org/faqs.htm

Pemmaraju, K. (2011, August 27). Let the Cloud Wars Begin: Who Will Be the Winners? Retrieved April 4, 2012, from Sandhill - Business Strategy for Software, Cloud and Mobile: http://sandhill.com/article/let-the-cloud-wars-begin-who-will-be-the-winners/

Perunovic, Z., & Pedersen, J. L. (2007). Outsourcing Process and Theories. Proceedings of the 18th Annual Conference of the Production and Operations Management Society. Dallas.

Ponemon Institute LLC. (2011). PERCEPTIONS ABOUT NETWORK SECURITY. Traverse City: Ponemon Institute.

PRC-FAQ. (2012). Retrieved January 13, 2012, from Privacy Rights Clearinghouse: http://www.privacyrights.org/data-breach-FAQ

Privacy Rights Clearinghouse. (2011, December 16). FAQ. Retrieved January 22, 2012, from Privacy Rights Clearinghouse.

Reehl, D. (2011). SSAE16.com - Service Organization Reports. Retrieved 9 8, 2011, from SSAE16.com: http://ssae16.com/SSAE16_reports.html

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: A Policy Framework for Information Security. Communications of the ACM , 46, 101-106.

Reilly, S. (2011, February 24). IT Management. Retrieved September 17, 2011, from ComputerWeekly.com: http://www.computerweekly.com/Articles/2011/03/02/245570/New-assurance-standard-required-for-cloud-confidence.htm

Reilly, S. (2011). New assurance standard is required to give cloud users more confidence. Computer Weekly , 20.

Richard Kissel, E. (2011, February). Glossary of Key Information Security Terms. Retrieved September 14, 2011, from NIST - Computer Security Division - Publications: http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

SAS70.com. (2011). SAS70 Overview. Retrieved 9 6, 2011, from SAS70.com: http://sas70.com/sas70_overview.html

Shared Assessments. (2011). About. Retrieved October 18, 2011, from Shared Assessments: http://www.sharedassessments.org/about/

Siponen, M. T. (2001). An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications. In G. Dhillon, Information Security

Management: Global Challenges in the New Millennium (pp. 102-128). Hershey, PA: Idea Group.

Stevens, J. P. (2002). Applied Multivariate Statistics for the Social Sciences (4th ed.). Mahwah: Lawrence Erlbaum Associates, Inc.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications , 34, 1-11.

Subramanian, K. (2010, October 19). CloudAve Home. Retrieved October 24, 2011, from CloudAve: http://www.cloudave.com/6819/cloudaudit-joins-csa/

The Higher Ed CIO. (2011, September 2). Cloud Computing. Retrieved September 20, 2011, from The Higher Ed CIO: http://blog.thehigheredcio.com/2011/09/02/ssae-16-replaces-sas70/

U.S. SBA. (2011). FAQs: Frequently Asked Questions. Retrieved October 19, 2011, from U.S. Small Business Administration: http://web.sba.gov/faqs/faqindex.cfm?areaID=15

Venter, H. S., & Eloff, J. H. (2003). A taxonomy for information security technologies. Computers and Security , 22, 299-307.

Viega, J. (2009). Cloud computing and the common man. Computer , 42 (8), 106-108.

Vijayan, J. (2007, April 11). Computerworld Security Topics. Retrieved October 17, 2011, from COmputerworld.com: http://www.computerworld.com/s/article/9016296/Just_how_much_will_that_data_breach_cost_your_company_

Wailgum, T. (2009, January 26). GE Gets in the Cloud for New SaaS Supply Chain App. Retrieved September 27, 2011, from ITWorld Beta: http://www.itworld.com/saas/61383/ge-gets-cloud-new-saas-supply-chain-app

Wakefield, R. L., & Whitten, D. (2006). Examining User Perceptions of Third-Party Organization Credibility and Trust in an E-Retailer. Journal of Organizational and End User Computing , 1-19.

Wallace, L., Lin, H., & Cefaratti, M. A. (2011). Information Security and Sarbanes-Oxley Compliance:An Exploratory Study. Journal of Information Systems , 25 (1), 185-211.

Walsh, R. (2010, May). BKD Alerts. Retrieved September 24, 2011, from experience BKD: http://www.bkd.com/service/Assurance/Alerts/2010/2010-05alertsAA-1.htm

Wernerfelt, B. (1984). A resource-based view of the firm. Strategic Management Journal , 5, 171-180.

Whitman, M. E. (2003). Enemy at the Gate: Threats to Information Security. Communications of the ACM , 46, 91-95.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. International Journal of Information Management , 24, 43-57.

Zarkowski, J. D. (2010, July). SSAE 16 Replaces SAS 70 as the New Standard for Service Auditors. Wall Street Argus . New York, New York, USA: Rothstein, Kass & Company.

List of Appendices

Appendix 1

Appendix 1 – Survey Instrument

Hello.

My name is Eric Sims. I am conducting research that attempts to identify factors that could make data more secure in a cloud computing environment.

Successful completion of this project may benefit the entire distributed-computing world (and will also help me obtain my PhD).

Would you please take a moment to help with this important research and become a valuable contributor to the solution?

To participate, simply "reply" to this email and type an "X" (or the year, where appropriate) into the blanks by your answers. If you prefer not to participate, simply delete this email. Either way, I thank you very much for your time.

CLOUD-BASED SERVICES SURVEY

1. Does your company consume any cloud-based services?

___Yes___No

2. If yes, please specify which cloud-based services you employ by indicating what year you implemented them.

APPLICATION (Indicate Year Deployed)

Monitoring_____
Content_____
Collaboration_____
Communication_____
Finance_____

PLATFORM (Indicate Year Deployed)

Object Storage_____
Identity_____
Runtime_____
Queue_____
Database_____

INFRASTRUCTURE (Indicate Year Deployed)

Compute_____
Block Storage_____
Network_____

3. Are your current cloud service provider's data handling procedures audited by a CPA?

___Yes___No___Unknown

If yes, what type of report was issued?

___SAS70/SSAE16
___AICPA SOC report: ___Type 1 ___Type 2 ___Type 3
___Unknown

4. Have you ever experienced a data breach with any:

a. Non-SAS70/SSAE16/SOC datacenter-hosted systems?

___Yes___No

b. SAS70/SSAE16/SOC datacenter-hosted systems?

___Yes___No

5. If either 4a or 4b is yes, are you still willing to host your critical business functions in the cloud?

___Yes___No

Why or why not?

6. How important is SAS70/SSAE16/SOC certification to your decision?

(Please place an X on the line below)

Not at all Important 1-2-3-4-5-6-7-8-9 Critical

7. Are you familiar with the differences in the assurance provided by SOC Type 2 and Type 3 reports versus SAS70/SSAE16/SOC-Type 1 reports?

___Yes___No

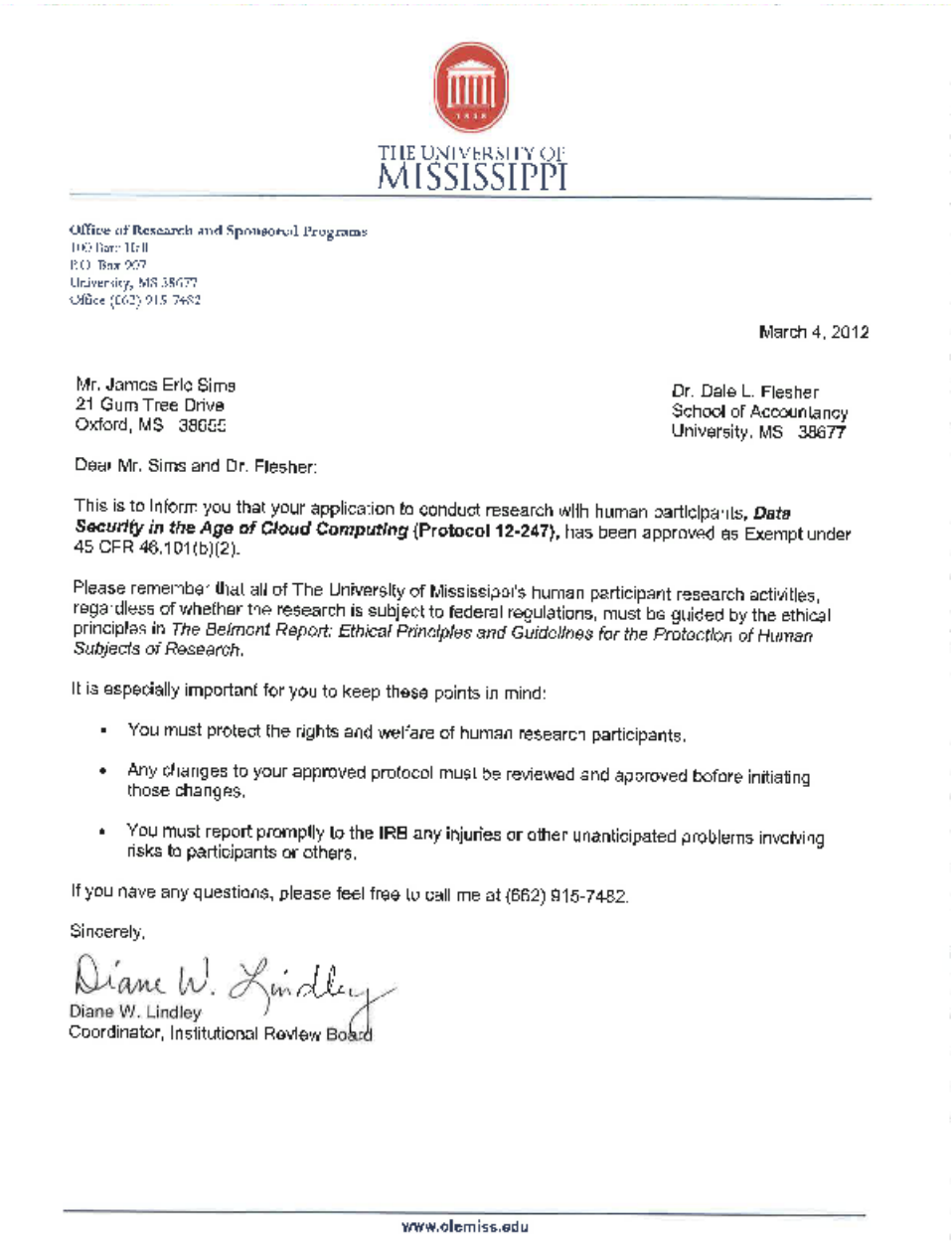
Any additional comments regarding your experience with or thoughts on data security in a cloud environment would be greatly appreciated.

Thank you very much for your participation in this research study.

This study has been reviewed by The University of Mississippi's Institutional Review Board (IRB). The IRB has determined that this study fulfills the human research subject protections obligations required by state and federal law and University policies. If you have any questions, concerns, or reports regarding your rights as a participant of research, please contact the IRB at (662) 915-7482.

Appendix 2

Appendix 2 – IRB Approval



THE UNIVERSITY OF MISSISSIPPI

Office of Research and Sponsored Programs
[illegible]
P.O. Box 997
University, MS 38677
Office (662) 915-7482

March 4, 2012

Mr. James Eric Sims
21 Gum Tree Drive
Oxford, MS 38655

Dr. Dale L. Flesher
School of Accountancy
University, MS 38677

Dear Mr. Sims and Dr. Flesher:

This is to inform you that your application to conduct research with human participants, ***Data Security in the Age of Cloud Computing*** **(Protocol 12-247),** has been approved as Exempt under 45 CFR 46.101(b)(2).

Please remember that all of The University of Mississippi's human participant research activities, regardless of whether the research is subject to federal regulations, must be guided by the ethical principles in *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research.*

It is especially important for you to keep these points in mind:

- You must protect the rights and welfare of human research participants.
- Any changes to your approved protocol must be reviewed and approved before initiating those changes.
- You must report promptly to the IRB any injuries or other unanticipated problems involving risks to participants or others.

If you have any questions, please feel free to call me at (662) 915-7482.

Sincerely,

Diane W. Lindley

Diane W. Lindley
Coordinator, Institutional Review Board

www.olemiss.edu

Figure 19 - IRB Approval

Appendix 3

Appendix 3 – Monthly Data

MONTH * BRCH_TYP Crosstabulation

Count

		BRCH_TYP								Total
		DISC	HACK	CARD	INSD	PHYS	PORT	STAT	UNKN	
MONTH	Jan	49	42	5	30	36	75	19	11	267
	Feb	46	36	6	27	24	41	15	4	199
	Mar	37	51	7	34	25	69	15	7	245
	Apr	42	51	3	29	33	67	14	4	243
	May	34	53	6	27	33	58	13	9	233
	Jun	52	54	1	24	33	67	16	12	259
	Jul	46	46	2	27	32	71	9	6	239
	Aug	40	47	4	22	38	78	17	11	257
	Sep	38	39	3	29	27	62	20	3	221
	Oct	40	26	1	14	32	85	17	9	224
	Nov	39	33	3	27	24	58	20	6	210
	Dec	42	56	0	26	32	74	16	4	250
Total		505	534	41	316	369	805	191	86	2,847

Table 30 – Breaches by Type by Month

Appendix 4

Appendix 4 – Annual Data

YEAR * BRCH_TYP Crosstabulation

Count

		BRCH_TYP								
		DISC	HACK	CARD	INSD	PHYS	PORT	STAT	UNKN	Total
YEAR	2005	20	48	0	10	8	38	10	2	136
	2006	83	75	3	32	39	186	48	16	482
	2007	98	71	2	23	43	163	36	16	452
	2008	79	57	5	31	53	99	22	9	355
	2009	53	53	4	30	38	61	10	4	253
	2010	97	97	13	104	103	142	37	12	605
	2011	75	133	14	86	85	116	28	27	564
Total		505	534	41	316	369	805	191	86	2,847

Table 31 - Breaches by Type by Year

Appendix 5

Appendix 5 – Breach Type by Org Type Data

BRCH_TYP * ORG_TYP Crosstabulation

Count

		ORG_TYP							
		BSO	BSF	BSR	EDU	GOV	MED	NGO	Total
BRCH_TYP	DISC	49	50	30	166	142	63	5	505
	HACK	92	66	109	175	52	28	12	534
	CARD	2	17	22	0	0	0	0	41
	INSD	38	64	41	14	59	96	4	316
	PHYS	37	46	27	46	89	116	8	369
	PORT	104	125	49	118	145	236	28	805
	STAT	20	23	11	47	21	64	5	191
	UNKN	12	21	9	12	16	13	3	86
Total		354	412	298	578	524	616	65	2,847

Table 32 - Breach Type by Organization Type

Appendix 6

Appendix 6 – Non-Significant Trends by Breach Type

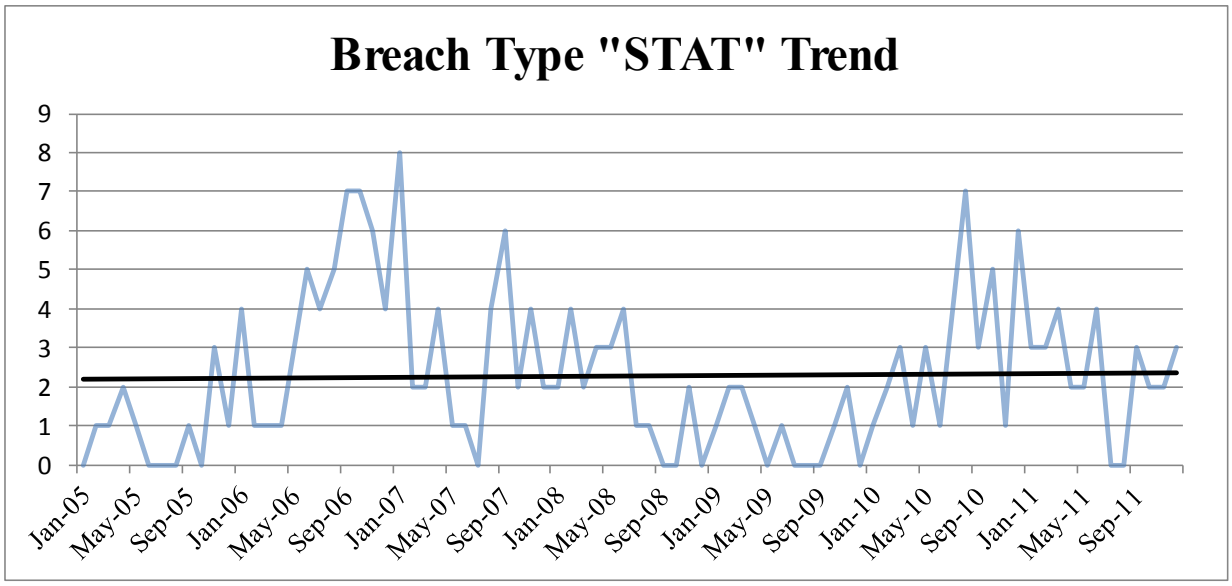


Figure 20 - "Stationary Device" Trend

There is no noticeable trend for the "STAT" breach type, as seen in Figure 20. Note that the Phi coefficient confirms the lack of significance (*Phi coefficient* = .190, p = .068) in Table 33.

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	102.905	83	.068
Likelihood Ratio	110.235	83	.024
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.190**	**.068**
	Cramer's V	.190	.068
N of Valid Cases		2,847	

Table 33 – Non-significant "Stationary Device" Trend

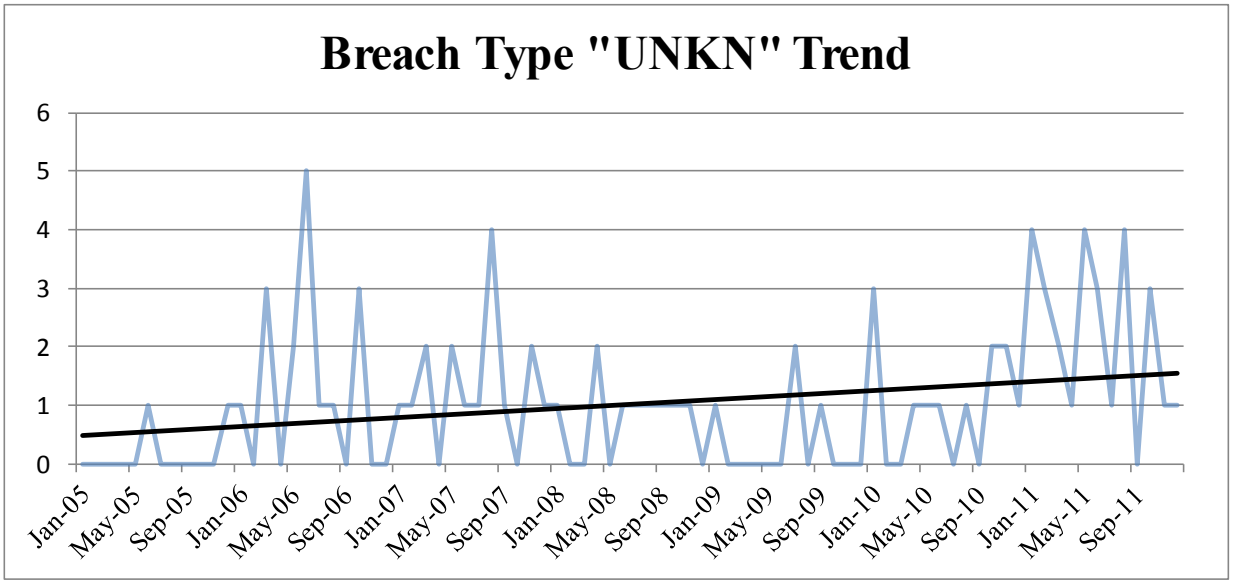


Figure 21 - "Unknown" Trend

As is the case with the "STAT" breach type, there is no significant trend in the breach frequency in the "UNKN" category. This is not so obvious in the graph in Figure 21, but it is confirmed by Table 34 (*Phi coefficient* = .173, p = .418).

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	85.029	83	.418
Likelihood Ratio	97.561	83	.131
N of Valid Cases	2,847		

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	**Phi**	**.173**	**.418**
	Cramer's V	.173	.418
N of Valid Cases		2,847	

Table 34 - Non-significant "Unknown" Trend

Appendix 7

Appendix 7 – Breach and Organization Frequency Data

BRCH_TYP

	Frequency	Percent	Valid Percent
DISC	505	17.7	17.7
HACK	534	18.8	18.8
CARD	41	1.4	1.4
INSD	316	11.1	11.1
PHYS	369	13.0	13.0
PORT	805	28.3	28.3
STAT	191	6.7	6.7
UNKN	86	3.0	3.0
Total	2,847	100.0	100.0

Table 35 - Supporting Data for Figure 10

ORG_TYP

	Frequency	Percent	Valid Percent
BSO	354	12.4	12.4
BSF	412	14.5	14.5
BSR	298	10.5	10.5
EDU	578	20.3	20.3
GOV	524	18.4	18.4
MED	616	21.6	21.6
NGO	65	2.3	2.3
Total	2,847	100.0	100.0

Table 36 - Supporting Data for Figure 11

Appendix 8

Appendix 8 – Hypothesis 4 Supporting Tables

Organization Type "Business, Other"

		Frequency	Percent	Valid Percent
Valid	DISC	49	13.8	13.8
	HACK	92	26.0	26.0
	CARD	2	0.6	0.6
	INSD	38	10.7	10.7
	PHYS	37	10.5	10.5
	PORT	104	29.4	29.4
	STAT	20	5.6	5.6
	UNKN	12	3.4	3.4
	Total	354	100.0	100.0

Table 37 - Supporting Data for Figure 12

Organization Type "Business, Financial & Insurance"

		Frequency	Percent	Valid Percent
Valid	DISC	50	12.1	12.1
	HACK	66	16.0	16.0
	CARD	17	4.1	4.1
	INSD	64	15.5	15.5
	PHYS	46	11.2	11.2
	PORT	125	30.3	30.3
	STAT	23	5.6	5.6
	UNKN	21	5.1	5.1
	Total	412	100.0	100.0

Table 38 - Supporting Data for Figure 13

Organization Type "Business, Retail/Merchant"

		Frequency	Percent	Valid Percent
Valid	DISC	30	10.1	10.1
	HACK	109	36.6	36.6
	CARD	22	7.4	7.4
	INSD	41	13.8	13.8
	PHYS	27	9.1	9.1
	PORT	49	16.4	16.4
	STAT	11	3.7	3.7
	UNKN	9	3.0	3.0
	Total	298	100.0	100.0

Table 39 - Supporting Data for Figure 14

Organization Type "Educational Institutions"

		Frequency	Percent	Valid Percent
Valid	DISC	166	28.7	28.7
	HACK	175	30.3	30.3
	INSD	14	2.4	2.4
	PHYS	46	8.0	8.0
	PORT	118	20.4	20.4
	STAT	47	8.1	8.1
	UNKN	12	2.1	2.1
	Total	578	100.0	100.0

Table 40 - Supporting Data for Figure 15

Organization Type "Government/Military"

		Frequency	Percent	Valid Percent
Valid	DISC	142	27.1	27.1
	HACK	52	9.9	9.9
	INSD	59	11.3	11.3
	PHYS	89	17.0	17.0
	PORT	145	27.7	27.7
	STAT	21	4.0	4.0
	UNKN	16	3.1	3.1
	Total	524	100.0	100.0

Table 41 - Supporting Data for Figure 16

Organization Type "Medical/Healthcare Providers"

		Frequency	Percent	Valid Percent
Valid	DISC	63	10.2	10.2
	HACK	28	4.5	4.5
	INSD	96	15.6	15.6
	PHYS	116	18.8	18.8
	PORT	236	38.3	38.3
	STAT	64	10.4	10.4
	UNKN	13	2.1	2.1
	Total	616	100.0	100.0

Table 42 - Supporting Data for Figure 17

Organization Type "Nonprofit Organizations"

		Frequency	Percent	Valid Percent
Valid	DISC	5	7.7	7.7
	HACK	12	18.5	18.5
	INSD	4	6.2	6.2
	PHYS	8	12.3	12.3
	PORT	28	43.1	43.1
	STAT	5	7.7	7.7
	UNKN	3	4.6	4.6
	Total	65	100.0	100.0

Table 43 - Supporting Data for Figure 18

Appendix 9

Appendix 9 – Tables for Hypothesis 6 Testing

Table 44 confirms that there are only 11 observations that fit the criteria for testing of Hypothesis 6.

SQ5 * SQ6 Crosstabulation

Count

		SQ6					
		1	3	4	8	9	Total
SQ5	0	3	1	0	1	1	6
	1	1	1	1	1	1	5
Total		4	2	1	2	2	11

Table 44 – Future Intent versus Importance Placed on Assurance Services (Hypothesis 6)

Table 45 provides the Chi-square result and Table 46 presents the binary logistic regression result for the tests performed on this very limited sample. No conclusions should be attributed to these results.

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	.346	1	.557
	Block	.346	1	.557
	Model	.346	1	.557

Table 45 – Hypothesis 6 Chi-square Result

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	SQ6	.109	.188	.339	1	.560	1.115
	Constant	-.664	1.035	.411	1	.521	.515

a. Variable(s) entered on step 1: SQ6.

Table 46 – Hypothesis 6 Binary Logistic Regression Result

Appendix 10

Appendix 10 – Tables for Hypothesis 7 Testing

Table 47 indicates that only 12 observations were available for testing of Hypothesis 7.

SQ5 * SQ7 Crosstabulation

Count

		SQ7		
		0	1	Total
SQ5	0	4	2	6
	1	3	3	6
Total		7	5	12

Table 47 – Future Intent versus Assurance Knowledge Level (Hypothesis 7)

Table 48 provides the Chi-square result and Table 49 presents the binary logistic regression result for the tests performed on this very limited sample. No conclusions should be attributed to these results.

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	.345	1	.557
	Block	.345	1	.557
	Model	.345	1	.557

Table 48 – Hypothesis 7 Chi-square Result

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	SQ7	.693	1.190	.339	1	.560	2.000
	Constant	-.288	.764	.142	1	.706	.750

a. Variable(s) entered on step 1: SQ7.

Table 49 – Hypothesis 7 Binary Logistic Regression Result

VITA

J. Eric Sims, PhD, CPA, CMA
Assistant Professor of Accounting
1000 East University Avenue, Dept. 3275
Laramie, WY 82071
307.766.3136
acctdept@uwyo.edu

EDUCATION:

Master of Accountancy, University of Central Arkansas, Conway, 2007.

Bachelor of Arts, Accounting & Accounting Information Systems (Dual Major, Minor in Finance). University of West Florida, Pensacola, 1990.

TEACHING EXPERIENCE:

Graduate Assistant, 2008 – 2011
University of Mississippi, Oxford, MS
Courses: Financial Accounting
Managerial Accounting (8 sections)
Accounting Information Systems (2 sections)

Adjunct Instructor, 2007 – 2008
University of Central Arkansas, Conway, AR
Courses: Managerial Accounting (2 sections)
Advanced Income Taxation
Intro to Economics

Adjunct Instructor, 2004 – 2005
Hillsborough Community College, Tampa, FL
Courses: Introduction to Accounting (2 sections)
Financial Accounting (3 sections)
Financial Management (2 sections)
Managerial Accounting (3 sections)

PROFESSIONAL EXPERIENCE:

Founder and Owner of my own CPA firm, 2002 – 2005
J. Eric Sims, CPA, Apollo Beach, FL
- Established business and developed client base
- Provided CPA services to business and individual clients
- Provided computer consulting services to businesses and individual clients
- Managed the business
- Practice was sold as a going-concern at a profit

Vice-President of Accounting and Finance, 2000 – 2001
Institute for International Research, Sarasota, FL
- Oversaw staff of thirty
- Provided accounting services to five separate corporations
- Reported to the president

Chief Financial Officer, 1995 – 2000
Mortgage Investors Corporation, St. Petersburg, FL
- Managed all accounting and finance functions
- Supervised a staff of twenty-five
- Offices in 46 states
- Reported to CEO

CPA & Assistant Network Administrator, 1993 – 1995
Kerkering, Barberio & Co., CPAs, Sarasota, FL
- Served CPA clients
- Assisted with the administration of a multi-location network, serving over fifty users
- Managed a computer consulting team to assist firm clients with their systems

CPA and Network Administrator, 1992 – 1993
Gregory, Sharer & Stuart, CPAs, St. Petersburg, FL
- Provided services to clients
- Maintained internal Novell network with more than thirty users
- Provided all in-house software training and support

Systems Analyst/Programmer, 1990 – 1992
Arthur Andersen & Co., Sarasota, FL
- Developed and tested computer software designed to aid tax preparers in Arthur Andersen field offices

Electronics Technician, 1982 – 1987
United States Air Force, Worldwide
- Maintained, serviced, diagnosed and repaired electronic radar equipment

PROFESSIONAL CERTIFICATIONS:

- Certified Public Accountant (CPA – license continuously active since 1992)
- Certified Managerial Accountant (CMA)

SCHOLARLY ACTIVITIES:

Working Papers:

- "*A Fresh Look at 'The Impact of Bonus Depreciation on General Aviation Aircraft Manufactured and Sold in the United States*", with Tonya K. Flesher.
- **"***Can Data Breach Frequency Be Decreased Through Enhanced Information Assurance Measures at Third-Party Service Providers?*"
- "*Effects of Plaintiff Type and Investment Loss on Jurors' Attributions of Negligence and Damages in Auditor Malpractice Litigation*", with Daniel C. Harris.
- "Market Reaction to Business Performance Management Implementation Announcements: An Event Study", with Mitchell R. Wenger.
- **"***Will Elimination of the Depreciation 'Loophole' Really Aid the Federal Debt-reduction Effort?*", with Karen C. Miller.

Presentations at Professional Meetings:

- "*A Fresh Look at The Impact of Bonus Depreciation on General Aviation Aircraft Manufactured and Sold in the United States*", with Tonya Flesher. American Accounting Association Southeast Region Meeting, Destin, Florida (April 9, 2011).

AWARDS AND HONORS:

University of Mississippi Graduate School Dissertation Fellowship – Spring 2012

SERVICE AND CONFERENCE ACTIVITIES:

AAA Annual Meeting, Denver, CO – August, 2011
Session moderator, AAA Southeast Regional Meeting, Destin, Florida – April 2011
Mid-South Doctoral Consortium, Oxford, MS – November 2010
Session moderator, AAA Southeast Regional Meeting, Oxford, Mississippi – April 2009
Mid-South Research Consortium, Starkville, MS – February 2009

PROFESSIONAL AFFILIATIONS:

American Accounting Association (AAA)
American Institute of Certified Public Accountants (AICPA)
Institute of Management Accountants (IMA)