An Investigation of Organizational Information Security Risk Analysis

by

Stephen Zachariah Jourdan

A dissertation submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Auburn, Alabama
May 14, 2010

Keywords: information systems, security, risk analysis, ISRA

Approved by

R. Kelly Rainer, Jr., Chair, Professor of Management Information Systems
Thomas E. Marshall, Associate Professor of Management Information Systems
F. Nelson Ford, Associate Professor of Management Information Systems

Abstract

From the dawn of the information age, technology has advanced rapidly to today where networked computers are almost ubiquitous. One of the problems with connecting computers together is the increased vulnerability to information security threats. Computer viruses, denial of service attacks, and intruders hacking into organizational information systems are becoming commonplace (Mitnick & Simon, 2002; Bodin, Gordon, & Loeb, 2005). In recent years, practitioners and researchers have begun to study issues related to information security (Straub & Welke, 1998). One component of this research is assessing the information security risk analysis practices of the organization (Cavusoglu, Mishra, & Raghunathan, 2004).

Despite a growing number and variety of information security threats, many organizations continue to neglect implementing information security policies and procedures. The likelihood that an organization's information systems can fall victim to these threats is known as information systems risk (Straub & Welke, 1998). To combat these threats, an organization must undergo a rigorous process of self-analysis. Rainer, Snyder, and Carr (1991) published one of the seminal papers related to Information Security Risk Analysis (ISRA). Since the publication of that work, very little research has been conducted to investigate the risk analysis processes that organizations conduct to assess and remedy the variety of information security threats that exist in a modern

networking environment. To better understand the current state of this information security risk analysis (ISRA) process, this study used two phase approach. In the first phase, a questionnaire using both open-ended and closed ended questions was administered to a group of information security professionals (N=32). The results of this initial investigation led to a second phase questionnaire where a regression model was tested using a new sample of information security professionals (N=144).

The qualitative and quantitative results of this study show that organizations are beginning to conduct regularly scheduled ISRA processes. However, the results also show that organizations still have room for improvement to create idyllic ISRA processes. In this exploratory study, a regression model was tested the effect of the frequency of the ISRA process, number of methodologies in the ISRA process, the use of insurance to protect the organization's information assets, the calculation of Return on Investment for security expenditures, the perceived significance of threats to the organization's information systems, the support of top management for the ISRA process, and the security culture of the organization all indicated a positive effect on the perceived ISRA effectiveness. Limitations of the study and implications for researchers and managers are discussed.

Acknowledgements

My deepest gratitude goes to my wife, Jessica. Her loving patience and kindness has helped me to complete this project. I am very thankful for my wonderful wife, and I dedicate this dissertation to her.

I would like to thank my wonderful dissertation chair, Dr. R. Kelly Rainer, Jr., for his encouragement and guidance seeing me through this project and the entire doctoral program. He always seemed to know when to push me to do more. I could not have asked for a better chairperson, friend, and mentor.

I would also like to thank my parents because they showed me, by example, to set and achieve goals. They always encouraged me to achieve my dreams, and for that I am truly in their debt.

I extend my gratitude to my committee members, Dr. Nelson Ford and Dr. Thomas Marshall, for their continuous support throughout my doctoral program. A special thanks to all professors who offered doctoral seminars for the students. Dr. Terry Byrd, Dr. William Boulton, Dr. Casey Cegielski, Dr. Christopher Craighead, Dr. Dianne Hall, Dr. Junior Feild, Dr. Allison Jones-Farmer, Dr. Alejandro Lazarte, and Dr. R. Kelly Rainer, Jr. provided seminars that laid the foundation for my career in academia, and I thank them for that.

Table of Contents

List of Tables

List of Figures

CHAPTER I

INTRODUCTION

From the dawn of the information age, technology has advanced rapidly until today where networked computers are almost ubiquitous. A main concern with connecting computers together is that this increases an information system's exposure to information security threats. As a result of this exposure, computer viruses, denial of service attacks, and intruders hacking into organizational information systems are becoming commonplace (Mitnick & Simon, 2002; Bodin, Gordon, & Loeb, 2005). In recent years, society has become aware of computer-related security (i.e. information security) issues through stories in the popular news media. Computer viruses, identity theft, denial of service attacks, and incidents of informational espionage have become major news stories. Even when an organization is using firewalls, virus protection software, intrusion detection systems, and other advanced technologies, the organization's computers, networks, and information are not safe (Moore, 2003).

According to the 2007 CSI Computer Crime and Security Survey, "The average annual loss reported in this year's survey shot up to $350,424 from $168,000 the previous year. Not since the 2004 report have average losses been this high" (Richardson, 2007, p. 2). This level of security-related hazards is nothing new, but organizations have historically been oblivious to these dangers and have subsequently minimized

information security expenditures. This lack of security investment led Straub and Welke (1998) to state, "Information security concerns are often ignored by top managers, middle managers, and employees alike. As a result, many information systems are far less secure than they might otherwise be, and security breaches are far more frequent and damaging than is necessary" (Straub & Welke, 1998, p.2).

Even when top management supports the security initiatives, investments to protect against known vulnerabilities may not be sufficient to assure that an organization's information assets are safe. New threats are continuously being designed and deployed by cybercriminals to exploit vulnerabilities that defending organizations have not yet discovered. Extant literature has identified the advantages for these organizations to share information about new vulnerabilities, attacks, and damages from breaches (Ma & Pearson, 2005; Kotulic & Clark, 2004; Dutta & McCrohan, 2002). Yet, firms are hesitant to share security-related information. Information security related crime is responsible for a significant amount of financial loss to companies conducting business through the Internet (Gordon, Loeb, Lucyshyn, & Richardson, 2004). Internet-based attacks on corporate information assets, motivated by criminals with malicious intent, have been increasing in number and sophistication. However, the full degree of financial losses due to information security breaches is difficult to assess because the majority of organizations are hesitant to report breaches for fear of market reprisal (Campbell, Gordon, Loeb & Zhou, 2003).

In the current business environment, information systems security (InfoSec) has been proclaimed as a key issue for the development of a global Information Society

(Commission of the European Communities, 1994). Information security has attracted the attention of researchers, professionals, journalists, legislators, governments, and citizens. One would expect this publicity to raise awareness and lead organizations to invest in security. However, recent surveys show that the actual situation is rather frustrating.

Hinde (1998) analyzed the results of three recent surveys in the UK and compared them to the results of past surveys to conclude that "… the underlined messages of key risks; of lack of awareness; and of lack of preparedness by management have not altered since the very first UK Audit Commission Survey conducted in 1981". In addition to the lack of improvement, key results included the following: one in five organizations had suffered a serious breach of security; security policies were inadequate; there was a significant gap between awareness of security risks and steps taken to avoid them. Regarding the awareness to action gap, the Business Information Security Survey (Hinde, 1998) concluded that "… the regrettable truth is that people often know how to avoid security breaches and yet do nothing about it. According to the survey results, more than half of the organisations that had suffered security breaches felt they could have done something to prevent it" (Hinde, 1998).

Information technology (IT) professionals often find great difficulty in convincing corporate management to invest in security projects (Lindup, 1996). Corporate management usually supports projects that can prove their cost-effectiveness, follow stable and recognized methodologies that ensure their successful completion, demonstrate compliance with corporate strategic plan, and allow their effect on the organization to be

assessed. Even with these inherent barriers, organizations have taken these threats seriously and have begun to invest both technology and human resources to protect their information assets (Conry-Murray, 2003). Despite this effort, the pace of innovation by cybercriminals to exploit these vulnerabilities has increased. This development has made it more difficult for any single organization to be able to protect their network alone because information security is a complex technology-based ecosystem of attackers and defenders involved in a continuous learning process (Knapp, Morris, Rainer & Byrd, 2003).

In addition to this complex external environment, organizational strategy affects the role that information technology plays (Henderson & Venkatraman, 1993). At one extreme, emerging technology drives the strategy of the firm (Huber, 1990). At the other extreme, technology is merely a necessary tool to support operations (Carr, 2003). A firm's technological orientation (technological opportunism) drives investment to build the capability of identifying, assimilating, transforming, and exploiting emerging technology (Srinivasan, Lilien, & Rangaswamy, 2002). A firm's technological opportunism determines the degree that they choose to capitalize on emerging technologies such as the Internet. Leveraging Internet technology does not come without risks, including exposure to external attack. In an environment with scarce capital, organizations must decide how to allocate their resources to minimize this risk and protect themselves from security threats in the most cost effective way. The main goal of this study is to investigate this process.

Research Objective of the Study

Using both qualitative and quantitative methods, this study attempts to learn more about the analysis that organizations undergo to allocate their security resources. This process, information security risk analysis (ISRA), is a form of risk management undertaken to reduce the negative outcome of security breaches. These breaches threatening information assets take many forms. Threats can be external (i.e. viruses, cybercriminals, and natural disasters) or internal (i.e. human error, technical obsolescence, and ineffective security controls). With a seemingly infinite number of threats poised against information assets and a limited amount of financial resources and personnel, firms must choose which assets are most critical to the organization's survival. To protect the organization, choices must be made to balance risk factors such as maintaining legal requirements or the avoiding lawsuits from customers (Whitman, 2003). If a firm focuses too much on one factor, resources are being wasted that could be used to balance the risk posed by another threat. These ISRA processes are not holistic; these methods rely on a very simplistic model of the organization defined in terms of assets, mainly data, hardware, and software. This research attempts, for the first time, to determine the ISRA process in the context of the entire organization. Due to the very limited research about ISRA in the context of the entire organization, the researcher determined that an open-ended questionnaire would be the best methodology to begin the investigation of this process.

Organization of the Dissertation

The dissertation is organized into five chapters. Chapter I introduces the topic of Information Security Risk Analysis (ISRA). Chapter II provides a theoretical perspective by reviewing the relevant literature regarding the process investigated in this study. The chapter provides a literature background for ISRA. Chapter III covers the research methodology that explored the ISRA process. This chapter describes the six methodological steps of the project from survey creation to the creation of a proposed theoretical model. Chapter IV shows the results of testing the proposed regression model. Chapter V includes a discussion of the findings, major contributions, limitations of the study, and implications for research and practice. This discussion is followed by a conclusion to the study.

CHAPTER II

LITERATURE REVIEW

The first section of this chapter introduces the topic of information security and defines that as a separate concept from network security and computer security. The literature base for risk management is reviewed in the second section. The research for risk analysis in the information security context is discussed in the third section. The final section of Chapter II discusses the various ISRA approaches in detail.

Information Security

Information Security (InfoSec) is the set of processes, procedures, personnel, and technology charged with protecting an organization's information assets (Whitman and Mattord, 2003). These set of practices begin from the top of the organization with the senior executives analyzing the external environment and the current organizational structure to create the organization's strategy. The executives work together to with the head of each functional area (i.e. Chief Financial Officer, Chief Operating Officer, etc.) to create policies for their respective functional areas. The head of the Information Systems functional area, usually the Chief Information Officer (CIO), responds to this organizational mandate by creating the IS policy which dictates the structure of the organization's information systems and the policies of each department within the IS functional area. The CIO then works with the Chief Information Security Officer (CISO)

to create the InfoSec Policy as a subset of the IS function's policy (Whitman & Mattord, 2003; Rainer, Turban, & Potter, 2007). For a graphic depiction of this InfoSec Policy creation process, see Figure 1.

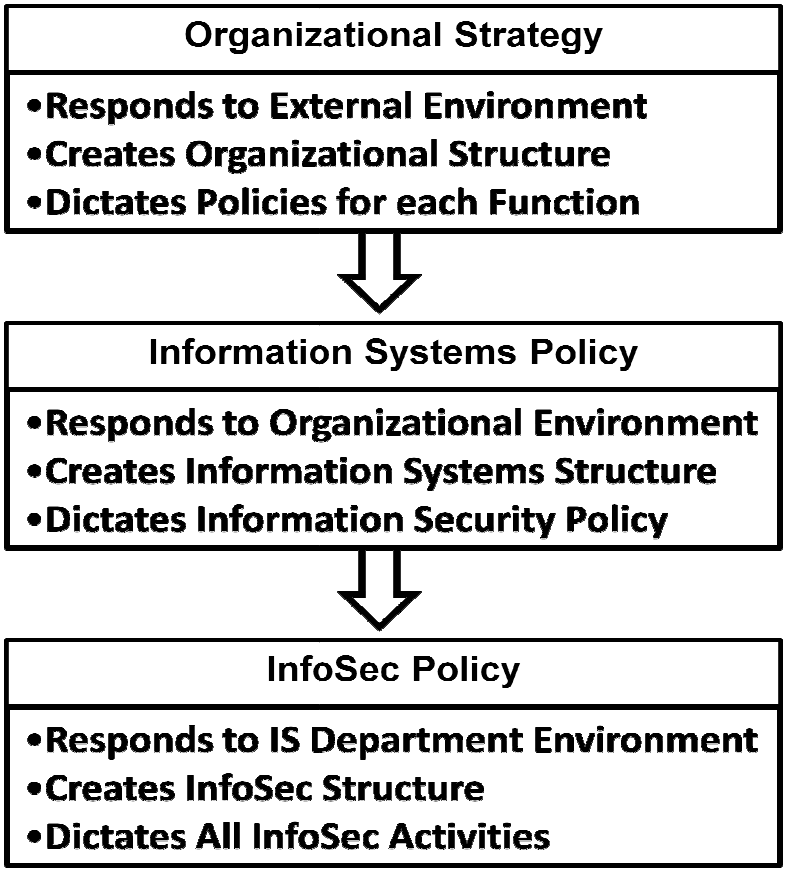


Figure 1. Development of InfoSec Activities

The InfoSec policy contains detailed plans and procedures for how the department will carry out all of the InfoSec activities. These activities include end-user training, operations, project management, risk management, and policy evaluation. End-user training is developed by the information security department to reduce the number of security-related incidents that occur through the users' lack of awareness. Operations deals with the day-to-day maintenance of current information security systems and all

other support activities. Project management deals with the creation and implementation of new security systems. Risk management is the process of identifying vulnerabilities to an information systems and taking action to control for those weaknesses. As new vulnerabilities appear, changes must be made to the organization's InfoSec policy to include these threats including contingency plans for incident response, disaster recovery, and business continuity planning (Whitman & Mattord, 2004). This study focuses on Risk Analysis as a subset of Risk Management depicted in Table 1.

Table 1. *InfoSec Practices* (Whitman & Mattord, 2004)

End-User Training	Information Security Education, Training and Awareness
Operations	Updating and maintaining current InfoSec systems
Project Management	Designing and implementing new InfoSec projects
Risk Management	Identifiying and controlling for risks to information assets
Policy Evaluation	Assessing current policy, making changes, contingency planning

Risk Management

Researchers and practitioners have longed stated that information technology (IT) projects were not secure from their inception. To deal with the complexities and uncertainties that increasingly surround technological change and its management, risk management can be an extremely powerful approach. Risk is sometimes seen as a negative concept with respect to IT in organizations because it implies that something could go wrong with an IT project. Conventionally, in IT projects, risks have been narrowly defined limited only to the financial success or failure associated with a

project's completion. Today, with IT becoming integral to a company's existence, the stakes are considerably higher and broader in scope (Smith, McKeen, & Staples, 2001).

The results of Smith et al.'s (2001) study, which involve a focus group of senior IT managers from a number of organizations in a variety of industries, were composed of the managers' presentations and a review of the current research on risk management. Smith et al. (2001) concluded that IT managers must learn to control both the problems and the potential that risk represents. The study developed several general principles to help IT managers deal effectively with these risks. Effective risk management involves taking a holistic approach to risk, developing a risk management policy, establishing clear accountabilities and responsibilities, balancing risk exposure against controls, being open about risks to reduce conflict and information hiding, enforcing risk management practices, and learning what works and what does not from past experience (Smith et al., 2001).

The underlying problem with risk is that managers are generally unaware of the full range of actions that they can take to reduce risk. Because of this lack of knowledge, subsequent actions to plan for and cope with risk are less effective. This is one viable explanation for why losses from computer abuse and computer disasters today are still so uncomfortably large and potentially devastating (Straub, 1998). An effective method for increasing an organization's knowledge of the risks and countermeasures associated with IT is to undergo some form of a risk analysis.

Risk Analysis

Rainer, Snyder, and Carr (1991) defined risk analysis (RA) as "the process managers use to examine the threats facing their IT assets and the vulnerabilities of those assets to the risks." (Rainer, Snyder, & Carr, 1991, p.133) Rainer et al. (1991) further stated that RA consisted of identifying assets, indentifying threats to those assets, and determining the vulnerability of said assets to those threats, and RA methodologies were either quantitative or qualitative. These methodologies would ideally be acceptable to all stakeholders (i.e. management, users, and the IS department), be comprehensive enough to assess all risks, be logically sound, be practical enough to deliver the best protection for the investment, and be conducive to learning through documentations and records of the RA process (Rainer, Snyder, & Carr, 1991).

Risk analysis (RA) is the predominant methodology for ISRA. Risk analysis is a rather straightforward methodology that follows the five stages of assets identification/valuation, threats assessment, vulnerabilities assessment, existing/planned safeguard assessment, and risk assessment (International Standards Organization, 2006). Baskerville (1991) stated that almost all information security professionals use RA for a tool to justify the cost of security controls to managment and attributes part of the success of RA to its use as a communication link between the security and management professionals who must take decisions concerning investments in InfoSec. "Its simple probability arithmetic allows the security problem to be expressed in a calculus that is familiar to management and in terms (monetary) that permit comparison with capital opportunity costs" (Baskerville, 1991, p.752).

Other researchers have attempted to improve upon this calculus. Gordon and Loeb (2002a) proposed an economic model composed of three parameters of a firm's expected loss due to information security breaches: the probability of a threat occurring, the probability that a threat would be successful (likelihood of a breach), and the loss resulting from a successful security breach. This model assigns the probability of a threat making the implicit assumption that all threats have an equal probability of occurring and the explicit determination that the firm cannot influence the probability of the occurrence of a threat. The model also assigns the value of the expected loss as a function of the probability of a breach. This logic makes the implicit assumption that firms are concerned with an average loss, instead of an extreme case.

Straub and Welke (1998) identify industry susceptibility to risk, past firm actions taken to secure information systems, and personal awareness of security risk as drivers for a manager's perception of risk. However, the study does not explicitly identify whether a firm's strategy influenced by technological opportunism has influence on the perception of security risk. Firms recognize that failure to carefully weigh action to address information security is important, because the market responds unfavorably to firms that spend either too much or too little to secure their information assets (Campbell et al., 2003). The prevailing wisdom is that investments in information security have been shown to have a diminishing return. (Gordon et al., 2002a) However, the problem is complex: "Normal tools utilized to evaluate investments such as ROI or IRR may not be appropriate" (Gordon & Loeb, 2002b, p. 28).

Investment to protect against known threats is necessary but not sufficient to guarantee security because the information security environment is, by definition, characterized by uncertainty. Firm investment can be categorized along a continuum of firm activism. At one end firms seek to transfer the risk through insurance or outsourcing contracts, and at the other end of the spectrum firms invest proactively in dynamic capabilities as a strategy to provide flexibility to address environmental uncertainty (Brealey, Myers, & Allen, 2005). Kogut and Kulatilaka (2001) identified lobbying the government as an additional form of proactive investment.

Even organizations that are proactive with respect to information security have reported uncertainty about the thoroughness of their preparations. The Computer Security Institute (CSI) stated in its 2007 report that the average annual loss reported by U.S. companies in the 2007 CSI Computer Crime and Security Survey more than doubled, from $168,000 in the 2006 report to $350,424 in the 2007 survey. This ends a five-year trend of lower reported losses (Richardson, 2007). Financial fraud overtook virus attacks as the source of the greatest financial loss. Virus losses, which had been the leading cause of loss for seven straight years, fell to second place. Another significant cause of loss was system penetration by outsiders. According to the results, almost one-fifth of those respondents who suffered one or more kinds of security incident said they had suffered a "targeted attack" (i.e. a malware attack aimed exclusively at their organization or at organizations within a small subset of the general population). Insider abuse of network access or e-mail (such as trafficking in pornography or pirated software) edged out virus incidents as the most prevalent security problem, with 59% and

52% of respondents reporting each respectively. At a period when experts throughout the industry have been discussing with concern the growing sophistication and stealth of cyber attacks, respondents are saying they lost significantly more money in 2006, as stated by Robert Richardson, CSI director and author of the survey (Richardson, 2007).

The study, by Campbell, Gordon, Loeb, and Zhou (2003), further illustrates the financial dangers associated with information security issues. The study examined the economic effect of information security breaches reported in newspapers or publicly traded US corporations. They found limited evidence of an overall negative stock market reaction to public announcements of information security breaches. However, further investigation revealed that the nature of the breach affected the result. Campbell et al. (2003) found a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach does not involve confidential information. Thus, stock market participants appeared to discriminate across types of breaches when assessing their economic impact on affected firms. These findings were consistent with the argument that the economic consequences of information security breaches vary according to the nature of the underlying assets affected by the breach (Campbell et al., 2003). To accomplish the goal of minimizing risk to information assets with a minimum investment, several ISRA approaches have been proposed.

Alternative ISRA approaches

In their paper, Rainer et al. (1991) categorized many RA methodologies into either the quantitative or qualitative categories. Annualized loss expectancy (ALE),

Courtney, Livermore Risk Analysis Methodology (LRAM), and Stochastic Dominance were all classified as expected value analysis where the loss exposure is a function of the asset's vulnerability to a threat multiplied by the likelihood of the reality of the threat using the Delphi method to solicit information and obtain consensus from users. These methodologies have the advantages of forcing the organization to identify their most vulnerable assets, develop contingency plans to operate without these assets, and test these plans to demonstrate how critical these assets are to the organization. The disadvantages of these methodologies are imprecision and cost. Measuring the probabilities of these assets being attacked by these threats is a very imprecise endeavour. While being inaccurate, the process can be very expensive in time, labor, and dollars invested (Rainer, Snyder, & Carr, 1991).

Rainer et al. (1991) described qualitative methodologies as an alternative to the more extensive quantitative methodologies. The qualitative methodologies include Scenario Analysis, Fuzzy Metrics, and questionnaires. As with the quantititative methodologies, the Delphi method could be used to clarify the variables under investigation. These methodologies have the advantages of being much less costly than the quantitative methods. However, the qualitative methodologies have the inherrent disadvantages of defininig risk in vague variables (i.e. low, medium, high, stong, weak, etc.) that do not provide exact dollar values and probalities (Rainer, Snyder, & Carr, 1991).

Since the publication of the study by Rainer, Snyder, and Carr (1991), other researchers have attempted to add to the portfolio of methodologies that an organization

can use for RA. Holbein, Teufel, and Bauknecht (1996) proposed the use of transaction-based business models for security design in organizations. These models are used to specify need-to-know authorizations and role-based access rights, based on information exchange and the client-supplier model. Backhouse and Dhillon (1996) rely on the conversational structures deriving from speech act theory (Searle, 1987) to propose a theoretical and conceptual foundation for analyzing IS security. They argue that an analysis of structures of responsibility in organizations may lead to the development of secure IS. These approaches support the analysis of the organization for the purpose of formulating specific security requirements. However, it has not been shown whether these can be used within a comprehensive ISRA methodology.

Badenhorst and Eloff (1989) have proposed an integrated methodology for ISRA. Their framework of a methodology for the life-cycle of computer security in an organization consists of the five phases of initiation, establishment of a computer security policy, risk analysis/project definition, installation, and maintenance. This methodology incorporates risk analysis into a comprehensive security framework. Organizational issues are addressed in the initiation stage. The second stage includes the development of a computer security policy, based on the mission statement of the organization, and the establishment of a computer security steering committee. However, this methodology does not include any kind of organizational analysis.

Hitchings' (1995) approach attempts to integrate risk analysis with organizational analysis in the context of a generic framework for ISRA. The proposed framework comprises the following phases:

1. Analysis of the organization and definition of relevant systems.
2. Security analysis of relevant systems.
3. Risk analysis.
4. Security design.
5. Security implementation, monitoring, and management.

In the first phase the organization is analysed to determine the systems that need to be examined from a security perspective. The second phase concerns the security analysis of these systems and includes the analysis of business processes and the interpretive analysis of information in the organization. Risk analysis is then performed in context to the organization. Security design, in the fourth phase, produces a security plan that includes a security policy and specific countermeasures. Finally, security implementation is coupled to monitoring and management. Monitoring and management are continuous activities that aim at keeping risk at a tolerable level (Hitchings, 1995). The weakness of this approach is that it views risk analysis as a step in a process, but the risk analysis is the entire process.

These initial attempts at an ISRA process are important attempts to develop workable security contols for the organization, and the quality of security controls can significantly influence all categories of risk. Traditionally, researchers and institutions recognized the direct impact from incidents related to fraud, theft, or accidental damage.

Many security weaknesses, however, can directly increase exposure in other areas. For example, the potential for legal liability related to customer privacy breaches may present additional risk. A strong information security program reduces levels of reputation, operational, legal, and strategic risk by limiting the institution's vulnerability to intrusion attempts and maintaining customer confidence and trust in the institution. Security concerns can quickly erode customer confidence and potentially decrease the adoption rate and rate of return on investment for strategically important products or services. Practitioners and risk managers should incorporate security issues into their risk analysis process for each risk category. Financial institutions should ensure that security risk assessments adequately consider potential risk in all business lines and risk categories.

Information security risk analysis is the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems. In its simplest form, a risk analysis consists of the identification and valuation of assets and an analysis of those assets in relation to potential threats and vulnerabilities, resulting in a ranking of risks (i.e. risk factors) to mitigate. The resulting information should be used to develop strategies to mitigate those risks. An adequate assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities. The next chapter illustrates the methodology used to gather more information about this complex business process.

CHAPTER III

RESEARCH METHODOLOGY

This research study combines quantitative and qualitative interviewing techniques using two phases. Quantitative interview studies attempt to report how many people are in particular categories and the relationships between one category and another. These studies, characterized by closed-ended Likert-scale questions, collect numbers as data, but this is not why these studies are quantitative. These studies, characterized by the sample survey, attempt to maximize the sample's generalizability to the population under investigation (Scandura & Williams, 2000). These studies are quantitative because all of their results can be presented as a table of numbers (Weiss, 1994).

In contrast, qualitative interview data tends to be narrative in nature. A qualitative interview produces rich, detailed answers while a quantitative interview is designed to produce data that can be coded and processed quickly. In qualitative interviewing the researcher is much more interested in the interviewee's point of view. This is in direct contrast to a structured quantitative interview where the researcher decides all of the questions and answers for the respondent (Bryman & Bell, 2003).

Researchers can combine quantitative and qualitative interview techniques in a study (Bryman & Bell, 2003). Figure 2 illustrates the two phases of the study combining

quantitative and qualitative interviewing techniques. The following sections provide detailed descriptions of the six methodological steps used in the two phases.

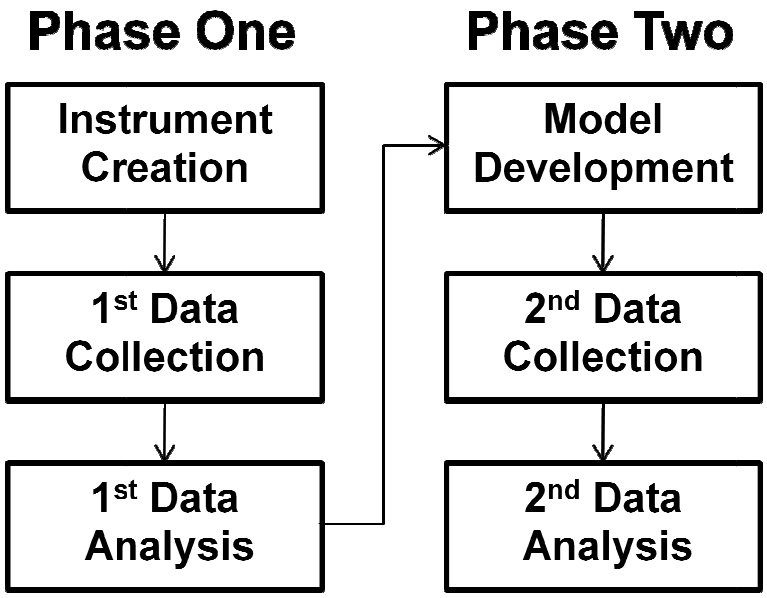


Figure 2. *Six Methodological Steps*

Step 1. Instrument Creation

The first phase of this methodology began by creating a survey instrument that would explore the complicated ISRA process. To accomplish this, an instrument was created by the principal researcher. Then, an expert panel including two accomplished university researchers and four Certified Information Systems Security Professionals (CISSPs) was consulted. CISSPs are members of the non-profit International Information Systems Security Certification Consortium who pass a comprehensive exam, agree to a code of ethics, possess a minimum level of professional experience, and earn continuing professional education credits (www.isc2.org). This expert panel reviewed

the questionnaire and suggested improvements regarding various aspects of the ISRA process including content validity and potential intrusiveness. Suggestions were made, changes implemented, and feedback was given in several stages over a two month period. After this iterative refinement process, the instrument was deemed ready for data collection.

Step 2. Phase One Data Collection

To initiate data collection, an email (see Appendix A) was sent to 300 CISSPs asking for their participation in a study being conducted by a researcher at Auburn University. The email explained the purposes of the study and assured possible participants that any information they provide was strictly anonymous and would only be used for research purposes. The email also explained that participation in the study required only that participants fill out a short survey, which would take between 20 and 30 minutes. Finally, the email directed those who desired to participate to download the attached spreadsheet, complete each part, and email the spreadsheet back to the researcher.

Those who did not respond to the first request for participation were contacted again with a second email. This second communication was sent approximately one week after the original communication and was the last time that non-responders were contacted. Finally, after two weeks the first phase of the data collection ended and the data was analyzed. Specifically, 300 individuals were contacted about participation in the study. Of the 300 individuals contacted, 32 completed the semi-structured survey for a response rate of 10.67%. A copy of the text for the semi-structured survey is included

in Appendix B. A screenshot of the Microsoft Excel worksheet is included in Appendix C.

Step 3. Phase One Data Analysis

The sample is notable for several reasons. First, the participants all had the CISSP certification (Table 2) indicating a standard of information securtity knowledge and experience. In addition to the CISSP certification, 25.1% of the participants held at least one additional information security related certification. Second, the CISSP certification is one of the most selective certifications in the information security profession, and individuals who earn this certification are held to the highest professional and ethical standards. Third, the sample of InfoSec professionals provided data from individuals who are highly knowledgeable about the ISRA process at their respective organizations. Finally, the holders of the CISSP certification work in a variety or information security roles in a diverse array of organizations.

Table 2. *Participants' InfoSec Certifications*

Please select your certification.	Response Percent	Response Count
None	0.0%	0
CISSP	100.0%	32
SSCP	18.8%	6
CAP	0.0%	0
Other	6.3%	2

CISSP Sample Characteristics

Table 3 illustrates the diversity with respect to number of employees, type of industry, job position, IT experience, and InfoSec experience. The sample had

participants who worked at a mix of small, medium, and large organizations. The respondents worked in a variety of industries in both the public and private sector. The professionals also worked in a variety of roles in the organization from rank and files workers represented by the Other IT/Technical/Scientific/Professional category through all levels of management from department head up to the owner and executive level of the organization. These professionals had a variety of IT and InfoSec experience with the vast majority being mid-level professionals with between six and fifteen years of experience.

Table 3. *Sample Characteristics of Phase One Respondents*

Employees:	More than 15,001	25.0%
	From 7,501 to 15,000	9.4%
	From 2,501 to 7,500	25.0%
	From 501 to 2,500	18.8%
	500 or less	21.9%
Industry:	*Largest represented include:*	
	Finance, Banking, & Insurance	18.8%
	Consultant	12.5%
	Information Technology/Security/Telecom	12.5%
	Manufacturing	12.5%
	Government-federal, military, local, etc.	6.3%
	Medical/Healthcare-public or private	6.3%
	Consumer Products/Retail/Wholesale	6.3%
	Utilities	6.3%
	Professional Services-Legal, Marketing, etc.	3.1%
	Education/Training	3.1%
	Energy	3.1%
	Publishing	3.1%
	Travel/Hospitality	3.1%
	Real Estate/Property Management	3.1%
Job Position:	Other IT/Technical/Scientific/Professional	40.6%
	MIS/IS/IT/Technical management	28.1%
	Consultant/Contractor	12.5%
	Department Manager/Supervisor/Director	9.4%
	Owner/Partner	6.3%
	Senior Manager/Executive	3.1%
IT Experience:	5 years or less	3.1%
	Between 6 and 10	43.8%
	Between 11 and 15	25.0%
	Between 16 and 20	15.6%
	More than 20	12.5%
InfoSec Experience:	5 years or less	31.3%
	Between 6 and 10	46.9%
	Between 11 and 15	12.5%
	Between 16 and 20	3.1%
	More than 20	6.3%

Table 4 further describes the participants. These professionals, mostly worked in North America represented by Canada and the United States, but a few other countries were also represented. The majority (78.1%) considered themselves permanent employees while 21.9% labeled themselves as an outsourced worker. Most of these professionals considered information security one of their primary job responsibilities.

Table 4. *Phase One Respondents' Country, Worker Status, & InfoSec Responsibility*

Select the country where you perform the majority of your work.	
United States – United States of America	68.8%
Canada	18.8%
United Kingdom	6.3%
Saudi Arabia – Kingdom of Saudi Arabia	3.1%
South Africa – Republic of South Africa	3.1%

Are you an outsourced (consultant) worker?	
YES, I'm an outsourced worker.	21.9%
NO, I'm a regular/permanent employee.	78.1%

Is information security a primary or secondary responsibility of current job?	
Primary	62.5%
Secondary	37.5%

Threat Significance

One of the critical tasks in the ISRA process is to identify threats and rank them according to significance. Organizations have limited resources with which countermeasures may be implemented. Whitman (2003) used a list of threats to determine whether organizations were concerned about the information security environment. That study resulted in a weighted ranking of threats that were similar to the

2002 CSI/FBI Annual Computer Crime and Security Survey (Whitman, 2003; Power, 2002). This questionnaire uses the same items and a 5-point Likert scale to ask participants to rank each threat's significance from extremely insignificant to extremely significant. The results, shown in Table 5, show that the vast majority (more than 90%) of participants listed acts of human failure, deliberate acts of espionage or trespass, deliberate acts of sabotage or vandalism, deliberate acts of theft, and deliberate software attacks as the most significant threats to their respective organizations.

Table 5. *Threat Significance by Percentage*

Threats	Extremely insignificant	Insignificant	Neither insignificant or significant
Act of human failure	0.0%	3.1%	6.3%
Compromises to intellectual property	3.1%	25.0%	9.4%
Deliberate acts of espionage or trespass	0.0%	9.4%	0.0%
Deliberate acts of information extortion	6.3%	15.6%	6.3%
Deliberate acts of sabotage or vandalism	3.1%	6.3%	0.0%
Deliberate acts of theft	0.0%	3.1%	0.0%
Deliberate software attacks	0.0%	9.4%	0.0%
Forces of nature	0.0%	12.5%	3.1%
Quality of service deviations from service providers	0.0%	21.9%	6.3%
Technical hardware failures or errors	0.0%	15.6%	6.3%
Technical software failures or errors	0.0%	21.9%	3.1%
Technical obsolescence	6.3%	31.3%	6.3%

Table 5 (continued). *Threat Significance by Percentage*

Threats	Significant	Extremely Significant
Act of human failure	37.5%	53.1%
Compromises to intellectual property	28.1%	34.4%
Deliberate acts of espionage or trespass	12.5%	78.1%
Deliberate acts of information extortion	15.6%	56.3%
Deliberate acts of sabotage or vandalism	21.9%	68.8%
Deliberate acts of theft	25.0%	71.9%
Deliberate software attacks	46.9%	43.8%
Forces of nature	46.9%	37.5%
Quality of service deviations from service providers	50.0%	21.9%
Technical hardware failures or errors	50.0%	28.1%
Technical software failures or errors	46.9%	28.1%
Technical obsolescence	25.0%	31.3%

Risk Factors

Baker, Rees, and Tippet (2007) stated that while organizations are attempting to take advantage of information technology to be competitive, those that do not pay heed to information security are actually making their organizations less competitive due to increased vulnerabilities. Management is faced with an array of information security standards and technologies, but no reliable criteria for making effective strategic decisions and determining the priority of those decisions regarding InfoSec expenditures. The Office of Homeland Security (2002) stated that a lack of real world data on how organizations set priorities on all the risks in a modern computing environment (i.e. risk factors). Table 6 shows that many organizations use some or all of the risk factors to plan their respective InfoSec strategies. When questioned about the Other category, these answers were more industry specific. Participants were concerned about violations of patient confidentiality in the medical industry, regulatory requirements in the financial services industry, and downstream liability in a variety of industries.

Table 6. *Risk Factors by Percentages*

When developing risk factors for your organization's risk analysis, which factors do your organization focus on the most?	Yes	No
Legal, regulatory, or statutory requirements	78.13%	21.88%
Loss of consumer confidence	75.00%	25.00%
Damage to organization's image/brand	78.13%	21.88%
Financial losses	93.75%	6.25%
Risks to infrastructure	81.25%	18.75%
Risks of possible lawsuits	71.88%	28.13%
Business requirements for information confidentiality, integrity, and availability	75.00%	25.00%
Other	25.00%	75.00%

Return on Investment for Information Security

The financial return for investing in information security counter measures has historically been difficult to calculate (Gordon & Loeb, 2002a; Gordon & Loeb, 2002b). Several strategies have been used in an attempt to place a dollar figure on a business concept that is difficult to quantify. The most common strategy is using fear, uncertainty, and doubt (FUD) to sell investments using anecdotal stories from real-world worst case scenarios. The second method is to estimate return on investment (ROI) for information security based on the cost of countermeasures. Another method is to use indirect estimates of the possible costs associated with security breaches. A more traditional approach involves using a traditional risk or decision analysis framework (Cavusolgo et al., 2004). This research project simply asked respondents whether their organization was using any method for the calculation of ROI for information security expenditures (Table 7). Of the respondents who stated their organization calculated ROI for information security, none would answer any follow up questions regarding the specifics of how their organization accomplishes this task. Several individuals specifically stated that they could not disclose that information due to the proprietary nature of that methodology.

Table 7. *ROI and Insurance for Information Security*

Does your organization calculate Return on Investment (ROI) for information security investments and expenses?	Response Percent
Yes	15.6%
No	84.4%
Does your organization purchase insurance to cover its information assets?	**Response Percent**
Yes	28.1%
No	71.9%

Insurance for Information Security

A minority of professionals (see Table XXX) indicated that their organization used insurance to protect their information assets. When further asked about the details regarding the insuring of their organization's information assets, respondents varied in the percentage of assets from the most critical assets only (10-15% of assets insured) to all information assets (90-100% of assets insured). The participants also indicated a wide variety of insurance strategies from traditional insurance, to outsourcing a variety of redundant services, to the establishment of a variety of cold, warm, and hot sites ready to go if disaster strikes. When these additional strategies were considered under the category of insurance, most participants agreed that their organization is using some form of insurance.

ISRA Frequency

When asked about the frequency of the ISRA process at their organizations, approximately one-fourth chose never or rarely for their department and organization (Table 8). The fact that this many organizations are conducting their ISRA process with

such haphazard infrequency is troubling. About half chose annually or quarterly chose either quarterly for their department and organization. The remainder chose Weekly/Monthly or Continuously for the frequency of their respective ISRA processes. When further probed about the frequency of the process at their organizations, individuals from this group made comments stating that this is an ongoing process with committees that meet regularly throughout the year.

Table 8. *ISRA Frequency*

How often is the information security risk analysis conducted for your department within your organization?	Response Percent
Never	9.4%
Rarely	15.6%
Annually	28.1%
Quarterly	12.5%
Weekly/Monthly	6.3%
Continuously	28.1%
How often is the information security risk analysis conducted for your entire organization?	**Response Percent**
Never	6.3%
Rarely	21.9%
Annually	25.0%
Quarterly	25.0%
Weekly/Monthly	3.1%
Continuously	18.8%

ISRA Participation and Approval

The expert panel was also curious to know who participated in the ISRA process. The expert panel hoped that the ISRA process was not simply delegated to the IT department and forgotten. The panel believed that when an organization used professionals, with a diverse knowledge of all the functional areas, a more successful

ISRA process could be achieved. Second, the panel also wanted to know if the ISRA process was achieving support from the executives and other managers in their respective organization. Finally, the panel was interested in knowing who had final approval of the ISRA process. The results of these queries are shown in Table 9.

Table 9. *ISRA Participation and Approval*

Which of the following individuals at your organization participate in information security risk analysis?	Yes	No
Owner/Partner	28.13%	71.88%
Senior Manager/Executive (e.g. CEO, CIO)	65.63%	34.38%
Department Manager/Supervisor/Director	87.50%	12.50%
MIS/IS/IT/Technical management	93.75%	6.25%
Other Managerial	68.75%	31.25%
Consultant/Contractor	84.38%	15.63%
Other IT/Technical/Scientific/Professional	87.50%	12.50%
Other Employees	40.63%	59.38%
Which of the following individuals at your organization have final approval of the information security risk analysis?	**Yes**	**No**
Owner/Partner	21.88%	78.13%
Senior Manager/Executive (e.g. CEO, CIO)	81.25%	18.75%
Department Manager/Supervisor/Director	40.63%	59.38%
MIS/IS/IT/Technical management	28.13%	71.88%
Other Managerial	6.25%	93.75%
Consultant/Contractor	9.38%	90.63%
Other IT/Technical/Scientific/Professional	6.25%	93.75%
Other Employees	6.25%	93.75%

Improved ISRA Process

As referred to earlier, many ISRA processes are available to the practitioner. These processes are developed by academics (Rainer et al., 1991; Holbein et al., 1996; Backhouse & Dhillon, 1996), government agencies (ISO, 2006; OHS, 2002) or

consultants hired by government agencies (Stoneburner, Goguen, & Feringa, 2002) in an attempt to give organizations a step-by-step process by which to conduct their ISRA. The expert panel attempted to develop a simple processes reflecting the best practices of a modern organization. The six-step process (Table 10) was met with great enthusiasm by the survey participants.

Table 10. *Proposed ISRA Process Agreement*

Step	Action
1	Determine IT assets
2	Determine value of IT assets.
3	Enumerate possible threats to IT assets.
4	Determine vulnerability of assets to specific threats.
5	Determine risk exposure for organization.
6	Minimize exposure and/or purchase insurance to minimize risk exposure.

Do you agree with the process above for information security risk assessment?	Response Percent
Yes	96.9%
No	3.1%

Despite this percent agreement, many participants noted that the six-step process did not contain a process to add new threats and reprioritize threats that were no longer important. Several other comments were made asking the researchers to consider the iterative ISRA process and how changes to the InfoSec policy were made as a result of the ISRA process. See Figure 3 for the proposed Information Security Risk Analysis methodology as part of a broad security risk management framework.

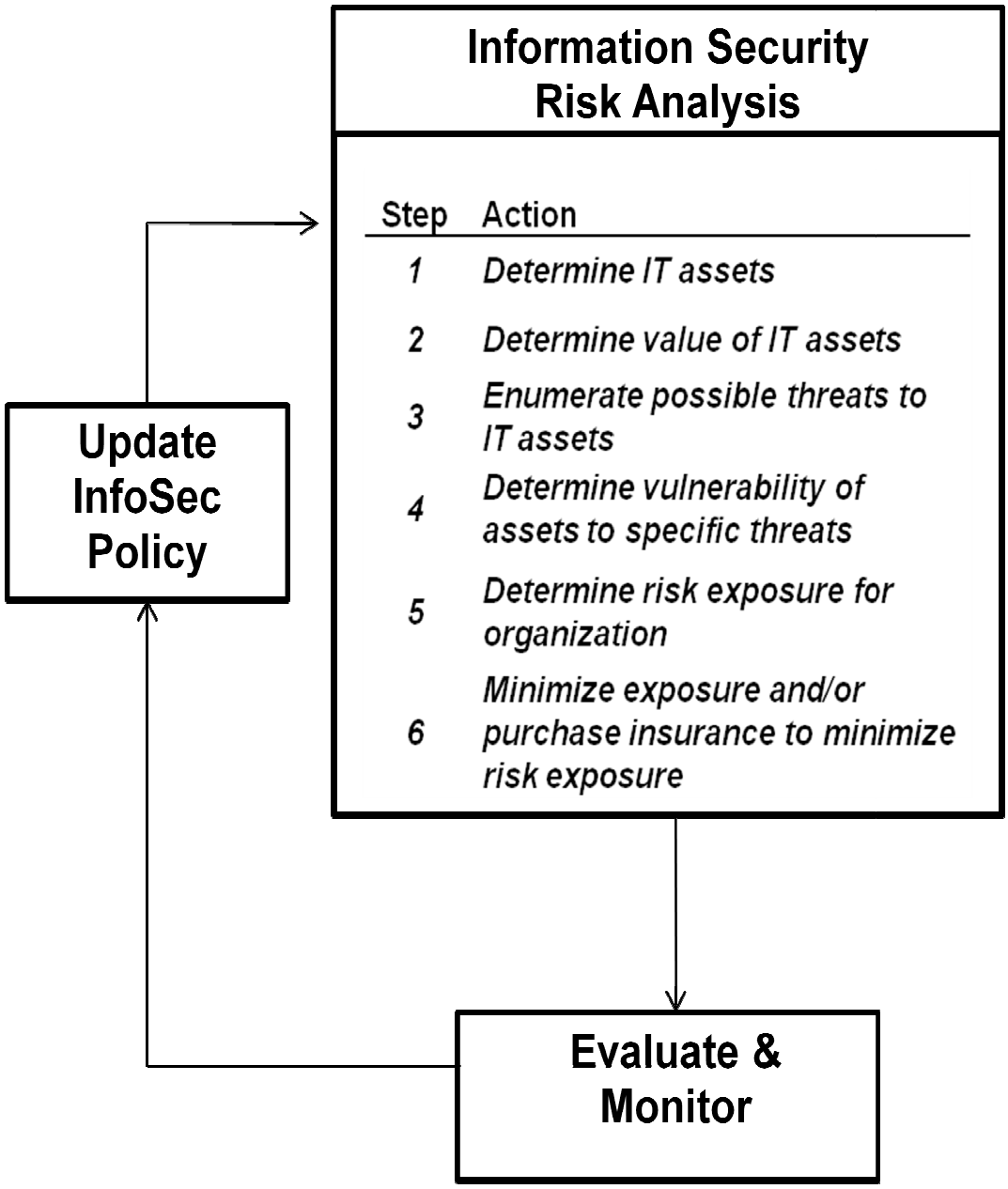


Figure 3. *Improved ISRA Process*

To develop the lists in the questionnaire, several sources were used. Beginning with a seminal work in ISRA (Rainer et al., 1991) and ending with the recent books on the subject (Whitman & Mattord, 2003; Whitman & Mattord, 2004), a fairly extensive list of methodologies were developed. The expert panel considered this a thorough list of methodologies used in the ISRA process and was interested to know how many were in use. As shown in Table 11, the information security risk assessment/auditing category, assessment of the routers, anti-virus software, and the use of firewalls were the most popular methodologies. The most popular methodologies to measure loss exposure were the Delphi technique/brainstorming, contractor assessments, single loss expectancy (SLE), questionnaires, and surveys. Another interesting fact was that many organizations relied on a variety of both qualitative and quantitative methodologies as encouraged by Rainer et al. (1991). In the Other category for both, a few respondents listed proprietary technologies and software not specifically listed in the questionnaire. However, upon further investigation, all of the answers given in the Other category could be classified in the categories listed on the survey.

Table 11. *ISRA and Loss Exposure Methodologies*

Select all information security risk assessment/audit methodologies used at your organization.	Yes	No
Anti-virus software analysis	90.63%	9.38%
Password cracking and improvement	84.38%	15.63%
Firewall implementation and correction of configuration errors	93.75%	6.25%
Vulnerability testing/correction	87.50%	12.50%
War dialing (scanning for unauthorized modems and fax machines)	59.38%	40.63%
Identification of critical infrastructure components	87.50%	12.50%
Physical security review	84.38%	15.63%
Centralized information storage location review	81.25%	18.75%
Access control evaluation	84.38%	15.63%
Certification identification	62.50%	37.50%
Integration of the firewall, VPN and e-commerce	65.63%	34.38%
Assessment of the routers and servers	93.75%	6.25%
Cryptography review	62.50%	37.50%
Computer Security Policy review and documentation	81.25%	18.75%
Other	25.00%	75.00%

Choose all the methodologies your organization uses to measure the possible loss exposure of information assets.	Yes	No
Consultant/Contractor Assessments	78.13%	21.88%
Annualized Loss Expectancy (ALE)	56.25%	43.75%
Courtney's ALE Method	21.88%	78.13%
Cost-Benefit Analysis (CBA)	56.25%	43.75%
Annualized Rate of Occurrence (ARO)	37.50%	62.50%
Single Loss Expectancy (SLE)	75.00%	25.00%
Livermore Risk Analysis Methodology (LRAM)	21.88%	78.13%
Stochastic Dominance/Daily Loss Formula	21.88%	78.13%
Scenario Analysis	65.63%	34.38%
Delphi technique/brainstorming	81.25%	18.75%
OCTAVE method	25.00%	75.00%
Fuzzy Metrics	21.88%	78.13%
Questionnaires	75.00%	25.00%
Surveys	75.00%	25.00%
Other	6.25%	93.75%

Step 4. Model Development

Throughout the first phase of this research project, a theme that emerged many times was the success (i.e. effectiveness) of the ISRA process. The literature contains no means of measuring the effectiveness of this complicated process because very few studies measuring effectiveness of any aspect of information security exist. One study attempted to measure user perceptions of concern for security as a measure of IS security effectiveness (Straub & Goodhue, 1991). Another developed a perceived measure of security effectiveness using responses about overall security deterrence, prevention, as well as the protection level of computer hardware, software, data, and services (Kankanhalli, Hock-Hai, Bernard, & Kwok-Kee, 2003). Another attempted to create a mediation model of information security effectiveness (Knapp, 2005).

In this study, the perceived ISRA effectiveness variable is based on the subjective judgment of security professionals and is directly based on the 5-item scale of Information Security Effectiveness (Kankanalli et al., 2003; Knapp, 2005; Knapp, 2006). Using self-reported, subjective measures has been frequently debated (Podsakoff & Organ, 1986; Straub, Boudreau, & Gefen, 2004). Despite the debate, self-reported, subjective measures can be an appropriate research tool for exploratory studies (Spector, 1994).

Frequency. Organizations that are successful at any initiative require practice to achieve success at that initiative, and that knowledge must be captured, organized, disseminated repeatedly due to the ever changing business environment (Davenport &

Prusak, 1998). A successful system for evaluating the threats to information assets at an organization occurs as an iterative process where the organization improves the quality of their security policies and procedures over time (Gordon & Loeb, 2006; Knapp, Marshall, Rainer, & Ford, 2006).

Hypothesis 1: The frequency of the information security risk analysis process will be positively related to their perceptions of information security risk analysis effectiveness.

Number of Methodologies. Rainer, Snyder, Carr (1991) warned organizations against using only one methodology to conduct the ISRA at their organization. A combination of different qualitative and quantitative methodologies will be the most effective strategy to manage the IT risks to organizations (Rainer, Snyder, & Carr, 1991). An economically based, formal process for evaluating the threats to information assets at an organization is not achieved without a combination of methodologies (Gordon & Loeb, 2006).

Hypothesis 2: The number of methodologies used in the information security risk analysis process will be positively related to their perceptions of information security risk analysis effectiveness.

Insurance for InfoSec. Organizations have long wanted to protect their information because the potential for substantial economic loss exists through the theft of proprietary information, natural disasters, and other potential attacks. Implementing expensive InfoSec countermeasures does not guarantee full protection. A new solution to this problem is cyber-risk insurance policies. These policies provide financial protection in the event of an information security breach, and organizations who are mature in their

ISRA process will lead their respective industries in this practice (Gordon, Loeb, & Sohail, 2003).

Hypothesis 3: The purchase of insurance to protect the organization's information assets will be positively related to their perceptions of information security risk analysis effectiveness.

ROI for InfoSec. Resources to invest information systems' resources are scarce in every organization, and when organizations allocate capital for any IT expenditure, the stakeholders need to be insured that outlay will be wise use of funds. Even now, many organizations have broken or non-existent ROI processes for information security expenditures (May, 1997). The organizations who have implemented metrics for their InfoSec expenditures will have the accountability offered by being able to measure where their security dollar may be invested with the most benefit (Cavusoglu et al., 2004).

Hypothesis 4: The calculation of Return on Investment (ROI) for the organization's information security investments will be positively related to their perceptions of information security risk analysis effectiveness.

Threat significance. Straub and Welke (1998) warned organizations to stop ignoring the threats to their organization's information assets. By not perceiving these threats as significant, organizations will have information systems that are far less secure than they could be. Without understanding the threats arrayed against the organizations, it is more likely that breaches will occur often and be costly when they do occur (Straub & Welke, 1998). Whitman (2003) took this one step further to encourage organizations to rank these threats as to their significance. Profiling the threats and knowing the threats

are the first steps in implementing countermeasures to fight the threat whether that threat is an individual, group, or force of nature (Whitman, 2003).

Hypothesis 5: Information security professional's perceptions of the significance of the threats against the organization's information systems will be positively related to their perceptions of information security risk analysis effectiveness.

Top Management Support. Another recurring topic of discussion in the qualitative phase of this project was the importance of having a management team that supported the ISRA process. Top management support is the degree that management believes in and allocates resources to the IS function (Ragu-Nathan, Apigian, Ragu-Nathan, & Tu, 2004). In the IS literature, the construct of top management support has been identified as the most frequently hypothesized variable contributing to IS implementation success (Markus, 1981; Sharma & Yetton, 2003). Top management (i.e. executives) significantly influence resource allocation and act as a champion of change to create a productive environment for successful IS implementation (Thong, Yap, & Raman, 1997). For four decades, top management support has been recognized as critical for effective computer security management (Allen, 1968; Wasserman, 1969; Parker, 1981). Dutta & McCrohan (2002) stated that effective organizational computer security does not start with firewalls or anti-virus software, but with top management support.

Hypothesis 6: Information security professional's perceptions of top management support for the information security risk analysis will be positively related to their perceptions of information security risk analysis effectiveness.

Security Culture. Culture can be defined as a set of beliefs, values, understandings, and norms shared by members of an organization (Daft & Marcic, 2001).

Culture has been an important topic in the practitioner literature (Santarelli, 2005) and has been identified as an opportunity for future IS research in security (Kankanhalli et al., 2003). The culture construct has been explored for its role regarding the implementation of new behaviors and organizational improvement initiatives (Detert, Schroeder, & Mauriel, 2000). In the IS literature, organizational culture has been examined as an opposition force resisting new technologies and transformations (Robey & Boudreau, 1999) and impacting organizational security (von Solms & von Solms, 2004).

Hypothesis 7: Information security professional's perceptions of the organization's security culture will be positively related to their perceptions of information security risk analysis effectiveness.

Table 12. *Summary of Proposed Hypotheses*

Hypotheses
1. The frequency of the information security risk analysis process will be positively related to their perceptions of information security risk analysis effectiveness.
2. The number of methodologies used in the information security risk analysis process will be positively related to their perceptions of information security risk analysis effectiveness.
3. The purchase of insurance to protect the organization's information assets will be positively related to their perceptions of information security risk analysis effectiveness.
4. The calculation of Return on Investment (ROI) for the organization's information security investments will be positively related to their perceptions of information security risk analysis effectiveness.
5. Information security professional's perceptions of the significance of the threats against the organization's information systems will be positively related to their perceptions of information security risk analysis effectiveness.
6. Information security professional's perceptions of top management support for the information security risk analysis will be positively related to their perceptions of information security risk analysis effectiveness.
7. Information security professional's perceptions of the organization's security culture will be positively related to their perceptions of information security risk analysis effectiveness.

In this study, a model was proposed and tested. The model consolidates the existing research on the information security risk analysis process and tests the relationship of several components of ISRA effectiveness. The model predicts that ISRA effectiveness is positively related to specific aspects of the frequency, the number of methodologies used, the purchase of insurance to protect information assets, the calculation of ROI for security expenditures, the significance of threats in the environment, the support of top management, and the culture of security at the organization. Figure 4 provides a depiction of the hypothesized model.

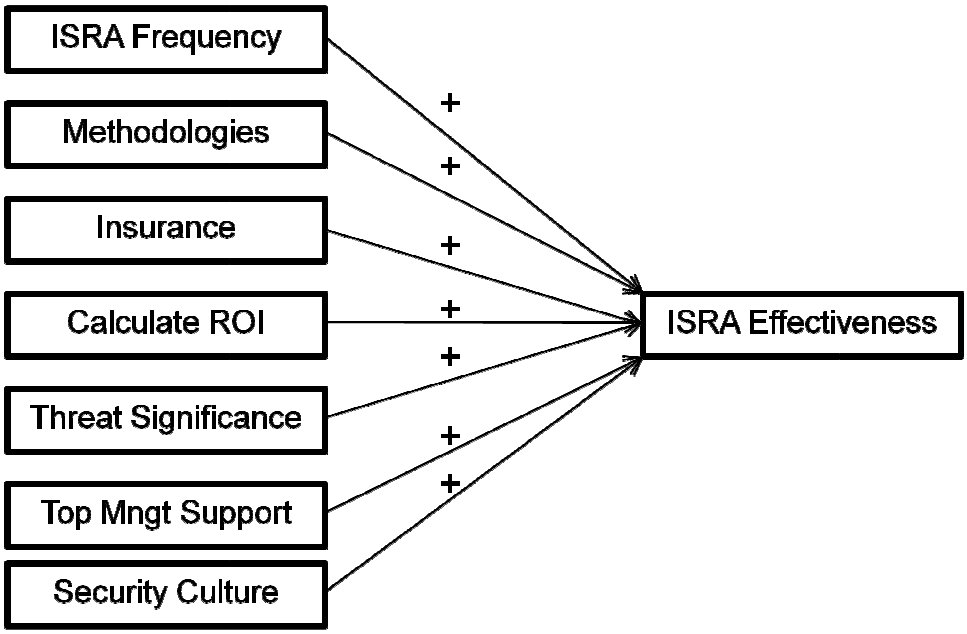


Figure 4. *ISRA Effectiveness Model*

Step 5. Phase Two Data Collection

Many concerns have been raised about using online web surveys in academic research. These concerns include constructing internet surveys, receiving incomplete or multiple responses, and managing confidentiality concerns (Simsek & Veiga, 2001;

Stanton & Rogelberg, 2001). The researcher used a popular online survey firm (SurveyMonkey) to develop the second phase online web survey. This software was designed with mechanisms in place to only allow fully completed surveys to be accepted, eliminating the need to discard incomplete surveys. The software only allowed participants to register for the survey one time, avoiding the danger of a single participant filling out multiple surveys. This list of email addresses was stored on a separate server to maintain the participants' confidentiality. Once the surveys were completed, the researcher received the data in formatted files that were easily loaded into SPSS. The survey did not need to be replicated using the internet web survey procedures outlined above. The data validation and collection procedures using internet surveys were much less labor intensive than when using traditional paper surveys.

Participants for the second phase of this study were recruited from lists obtained from a lead generation company that collects names of participants for marketing research. This company, Majon International, possessed lists of willing survey participants including information security professionals. As part of the service provided to the researcher, the company sent emails (see Appendix D), using their email system, to each potential participant in the second phase of the data collection.

An email was sent to each information security professional asking for their participation in a study being conducted by a researcher at Auburn University. The email explained the purposes of the study and assured possible participants that any information they provide was strictly anonymous and would only be used for research purposes. The email also explained that participation in the study required only that participants fill out

a short survey, which would take between 15 and 20 minutes. Finally, the email directed those who desired to participate to click the survey link and begin. Once a participant clicked the link, he or she was routed to the web survey and could begin entering information. After filling out the survey and clicking submit, participants were routed to a third page which thanked them for their helpful participation and reminded them that the information provided was strictly anonymous and would only be used for research purposes.

Those who did not respond to the first request for participation were contacted again with a second similar email. This second communication was sent approximately one week after the original communication and was the last time that non-responders were contacted. Finally, once a sufficient number of responses were received, the survey was taken off the web and the data was analyzed. Specifically, 1,000 individuals were contacted about participation in the study. Of the 1,000 individuals contacted, 144 completed the web survey for a response rate of 14.4%. A copy of the web survey is included in Appendix E.

Step 6. Phase Two Data Analysis

The phase two participants were similar to the respondents in the first phase (Table 3). Table 13 illustrates the diversity of this sample with respect to number of employees, type of industry, job position, IT experience, and InfoSec experience. The sample had participants who worked at a mix of small, medium, and large organizations. The respondents worked in a variety of industries in both the public and private sector. The professionals also worked in a variety of roles in the organization from rank and files

workers represented by the Other IT/Technical/Scientific/Professional category through all levels of management from department head up to the owner and executive level of the organization. These professionals had a variety of IT and InfoSec experience with the vast majority being mid-level professionals with between six and fifteen years of experience.

Table 13. *Sample Characteristics of Phase Two Participants*

Employees:	More than 5,000	59%
	From 501 to 5000	22%
	500 or less	19%
Industry:	*Largest represented include:*	
	Government-federal, military, local, etc.	22%
	Finance, Banking, & Insurance	13%
	Consumer Products/Retail/Wholesale	9%
	Medical/Healthcare-public or private	7%
	Manufacturing	6%
	Utilities	6%
	Information Technology/Security/Telecom	6%
	Education/Training	5%
	Non-Profit	4%
	Professional Services-Legal, Marketing, etc.	4%
	Transportation/Warehousing	4%
	Travel/Hospitality	4%
Job Position:	Consultant/Contractor	15%
	Department Manager/Supervisor/Director	10%
	MIS/IS/IT/Technical management	38%
	Other IT/Technical/Scientific/Professional	21%
	Other Managerial	3%
	Owner/Partner	5%
	Senior Manager/Executive	9%
IT Experience:	5 years or less	3%
	Between 6 and 10	33%
	Between 11 and 15	33%
	Between 16 and 20	26%
	More than 20	6%
InfoSec Experience:	5 years or less	39%
	Between 6 and 10	49%
	Between 11 and 15	10%
	Between 16 and 20	2%
	More than 20	0%

In addition to demographic data, information was collected on the organization's ISRA process. Questions relating to the frequency of the process, the methodologies used in the process, the use of insurance, the calculation of ROI for security expenditures, the significance of the threats, the support of top management, the security culture, and the effectiveness of the ISRA process. Table 14 contains each study variable and its definition. The means, standard deviations, intercorrelations, and coefficient alphas, when applicable, of all study variables are presented in Table 15.

Table 14. *Proposed Model Variables and Definitions*

	Study Variable	Definition
1	Frequency	Dummy variable coded as 1 if the organization conducts the ISRA process continuously, weekly, or monthly and 0 if the processes is completed less frequently
2	Methodologies	Dummy variable coded to 1 if the organization uses 6 or fewer methodologies, 2 for the inclusive range 7 to 12, 3 for 13 to 18, 4 for 19 to 24, and 5 for 25 or greater
3	Insurance	Dummy variable coded as 1 if the organization purchases insurance to protect its information assets and 0 if the organization does not
4	ROI	Dummy variable coded as 1 if the organization calculates return on investment for security investments to protect its information assets and 0 if the organization does not
5	Threat Significance	Average of the participant's answers rating the significance of 12 information security threats
6	Top Management Support	Average of the participant's answers to the 3 item Top Management Support scale
7	Security Culture	Average of the participant's answers to the 5 item Security Culture scale
8	ISRA Effectiveness	Average of the participant's answers to the 5 item ISRA Effectiveness scale

Table 15. *Means, Standard Deviations, Intercorrelations and Coefficient Alphas for Study Variables*

		Mean	SD	1	2	3	4
1	ISRA Effectiveness	3.994	1.050	1.000			
2	Frequency	0.285	0.453	0.581	1.000		
3	Methodologies	2.965	1.300	0.777	0.787	1.000	
4	Insurance	0.486	0.502	0.651	0.556	0.754	1.000
5	ROI	0.440	0.496	0.683	0.736	0.802	0.797
6	Threats	4.243	0.579	0.741	0.703	0.756	0.687
7	Top Mngt. Support	3.963	1.093	0.964	0.601	0.777	0.667
8	Security Culture	3.960	1.027	0.950	0.596	0.778	0.673

Table 15 (continued). *Means, Standard Deviations, Intercorrelations and Coefficient Alphas for Study Variables*

		5	6	7	8
1	ISRA Effectiveness				
2	Frequency				
3	Methodologies				
4	Insurance				
5	ROI	1.000			
6	Threats	0.760	1.000		
7	Top Mngt. Support	0.700	0.707	1.000	
8	Security Culture	0.737	0.712	0.942	1.000

Common Method Bias

Common Method Bias (CMB) is when the predictor and criterion variables are obtained from the same source, measured in the same context, and the source of the method bias cannot be identified (Podsakoff, MacKenzie, Lee, and Podsakoff, 2003). Podsakoff et al. (2003) stated that this bias is inherent in all survey research and provided a summary of sources and methods for dealing with common method problems. According to their work, the researcher should use all procedural remedies in survey design, separate the predictor and criterion variables psychologically, and guarantee response anonymity (Podsakoff et al., 2003). This study attempted to minimize the effects of CMB by carefully reviewing items to check for clarity of meaning, using scales with fewer items, removing headings in the survey instrument to remove potential priming effects, randomizing items to combat the social desirability effect, and all respondents were promised anonymity to encourage candid responses (Podsakoff et al., 2003). The proposed regression model and the results of the regression analysis of the proposed regression model are discussed in Chapter IV.

CHAPTER IV

RESULTS

Model Estimation

Taken together, the constructs and variables discussed in Chapter III allow the development of the following model.

$$Y = \beta_0 + \beta_1 (Freq) + \beta_2 (Meth) + \beta_3 (Ins) + \beta_4 (ROI) + \beta_5 (Threat) + \beta_6 (TMS) + \beta_7 (SC)$$

Where:

Y	=	Dependent variable, ISRA Effectiveness
Freq	=	Frequency of ISRA Process
Meth	=	Number of Methodologies
Ins	=	Purchase Insurance
ROI	=	Calculate ROI
Threat	=	Threat Significance
TMS	=	Top Management Support
SC	=	Security Culture

Results of Hypothesis Tests

Hypothesis 1 predicted a positive relationship between the frequency of the organization's ISRA process and the perceived effectiveness of the ISRA process. While the reported p-value is significant at .045, the results demonstrate a negative coefficient of -.150. Therefore, due to an inverse relationship, hypothesis one is not supported.

Hypothesis 2 predicted a positive relationship number of methodologies used in the information security risk analysis process and the perceived effectiveness of the ISRA process. The reported coefficient of .066 is positive and the reported p-value of .047 is significant at alpha level .05. Hypothesis 2 is supported.

Hypothesis 3 predicted a positive relationship between the purchase of insurance to protect an organization's information assets and the perceived effectiveness of the ISRA process. The reported p-value is not significant at .338, and the results demonstrate a negative coefficient of -.065. Therefore, hypothesis three is not supported.

Hypothesis 4 predicted a positive relationship between the calculation of ROI for an organization's information security expenditures and the perceived effectiveness of the ISRA process. While the reported p-value is significant at .014, the results demonstrate a negative coefficient of -.204. Therefore, due to an inverse relationship, hypothesis four is not supported.

Hypothesis 5 predicted a positive relationship between information security professional's perceptions of the significance of the threats against the organization's information systems and the perceived effectiveness of the ISRA process. The reported coefficient of .270 is positive and the reported p-value of .000 is significant at alpha level .05. Hypothesis 5 is supported.

Hypothesis 6 predicted a positive relationship between information security professional's perceptions of Top Management Support for the ISRA process and the perceived effectiveness of the ISRA process. The reported coefficient of .527 is positive

and the reported p-value of .000 is significant at alpha level .05. Hypothesis 6 is supported.

The last test, for Hypothesis 7, predicted a positive relationship between information security professional's perception of the security culture for the organization and the perceived effectiveness of the ISRA process. The results in this case support the hypothesis with a positive coefficient of .362 and a p-value of .000. Hypothesis 7 is supported. Table 16 provides a summary of the complete model results.

Table 16. *Table of Model Results*

Variable	Coefficient	Std Error	P-Value	Supported
Frequency of ISRA Process	-0.150	0.074	0.045*	No
Number of Methodologies	0.066	0.033	0.047*	Yes
Purchase Insurance	-0.065	0.068	0.338	No
Calculate ROI	-0.204	0.082	0.014*	No
Threat Significance	0.270	0.056	0.000*	Yes
Top Management Support	0.527	0.052	0.000*	Yes
Security Culture	0.362	0.057	0.000*	Yes

Note: * $p < .05$

The next chapter includes a discussion of the findings, major contributions, limitations of the study, and implications for research and practice. This discussion is followed by a conclusion to the study.

CHAPTER 5

DISCUSSION & CONCLUSION

The regression model constructed and tested in this study explains a large portion of the variance associated with security professional's perception of the effectiveness of the ISRA process at their organization reporting an R^2 of .937. Four of the variables measured were found to be significant: (a) Number of Methodologies, (b) Threat Significance, (c) Top Management Support, and (d) Security Culture. However, Hypothesis 3, dealing with the purchase of insurance, was not supported due to p-value which showed insignificance. Also, Hypotheses 1 and 4, dealing with the frequency of the ISRA process and the calculation of ROI respectively, were not supported due to directional inconsistencies.

Four hypotheses were supported with positive coefficients. The number of methodologies used in the ISRA process, the threat significance, top management support, and security culture all had a positive effect on perceived ISRA effectiveness. Organizations that use more methodologies likely have a more developed ISRA process. By comparison, a firm that is beginning its initial ISRA may be using only one or two methodologies. The veteran ISRA organizations that understand the severity and complexity of the threats would also be expected to work harder to a very thorough analysis. Alternatively, a novice organization would only be in the beginning stages of

learning about all possible threats and vulnerabilities. Top management support is crucial in this endeavour because this process uses organizational resources to do a professional job, and organizations where management withholds its support will not be able to complete all necessary ISRA activities due to budgetary concerns. An organization's security culture would also be critical to develop a successful ISRA process because all stakeholders would be vigilant for issues that could bring harm to an organization's information systems.

The frequency of the ISRA process and the calculation of ROI for security reported significant, yet negative coefficients. This is not what was hypothesized. This study will not attempt to demonstrate the cause of these negative relationships. However, a possible explanation for the negative relationship with frequency may be that information security professionals perceive that the effectiveness of the ISRA process does not necessarily dictate that organizations should conduct this process more frequently. An organization may achieve a high return on their security investment by conducting a thorough annual ISRA as opposed to a half-hearted monthly or quarterly affair. The survey participants may be more impressed with the quality of the processes regardless of the frequency.

Additionally, these professionals may be more focused on the security of the organization's information assets than financial measures like ROI. With experience, these professionals have likely seen expensive investments in information security countermeasures that yielded very little improvement in the organization's overall information security. These professionals have also likely seen great improvements in

the organization's information security with very little investment. The relationships between ISRA effectiveness, ISRA frequency, and information security ROI will need to be explored in future research projects.

Contributions of the Study

This study makes several contributions to the limited information security risk analysis body of knowledge. The ISRA process was investigated across a variety of industries. This investigation provided insight into ISRA process by using qualitative and quantitative data collection methods. A model for the ISRA process was developed and agreed upon by the professionals themselves. A list of risk factors for the ISRA process was developed and agreed upon by the professionals themselves. This study gained insight into the frequency of and participants in the ISRA process conducted across both the department and organization. A model for the broader framework of information risk management was introduced. In the context of the ISRA process, this study added to the knowledge of both managers and security professionals. Ma and Pearson (2005) stated that it was necessary to explore these interrelationships between management practices and security objectives. Future studies need to continue the exploration of this research stream to insure that organizations have the most efficient and effective ISRA process possible.

Limitations of the Study

This study has several limitations. First, this study only questioned security professionals that had obtained the CISSP designation. By focusing only on these security professionals, this study may have ignored the many competent information security professionals exist that do not have this certification. Many organizations may be conducting a competent ISRA process without a single CISSP on staff. Certain

industries may not even require this certification, and some organizations may even develop their own training for conducting this analysis. Second, the scope of the organizations involved in this study was broad in terms of industry sector (i.e. education, government, and business). Future studies may need to focus on a specific sector due to the likelihood that different industry sectors focus on different risk factors when determining their risk exposure. Finally, the sample size was not large enough to conduct a more thorough analysis of the quantitative data. Further investigation is required to develop techniques to collect data from information security risk analysis professionals in sufficient quantity to provide a more thorough and numerous data collection.

Implications for Research & Practice

In their 2004 study, Kotulic and Clark proposed a conceptual model based on the study of risk management at the firm level. Although considerable time and effort were expended in attempting to validate the usefulness of their proposed model, this effort was not successful. Kotulic and Clark (2004) provided a description of the problems faced while attempting to collect data from information security professionals. Research regarding an organization's information security practices is very intrusive. Information security professionals are, by nature, distrustful of anyone attempting to collect information about how they do their jobs. Kotulic and Clark (2004) sent out a mass mailing of 1540 unsolicited survey packages, and despite many efforts to solicit a response, received nine complete responses giving them a response rate of .61%. The authors went on to state that it is nearly impossible to collect information security data from an organization without a major supporter. This research project faced similar

obstacles, but this non-response issue was remedied by targeting information security professionals who have opted to receive questionnaires from researchers. Using this strategy, this research project did achieve a favorable response rate. Until researchers find creative ways to reach these nervous participants, who do not feel safe to disclose security information about their respective organizations, the growth of the information security body of knowledge is going to be hampered by failed research projects.

Managers who are serious about protecting their organization's information assets need to ensure that a thorough organizational information security risk analysis is being conducted at their organization. With top management support, the information security professionals cannot develop and maintain processes that identify new threats, protect the organizations assets from existing threats, and develop dynamic and thorough security policies to develop an organizational culture with security as on of its core values. Considering the dangers and costs associated with security incidents, it is critical today for organizations to take this process seriously in order to secure their valuable information assets.

Conclusion of the Study

This research effort has made a significant contribution to the information security risk analysis body of knowledge, but much work remains. Judging by the high volume of threats to information security assets, the value of a competent ISRA process will continue to grow across a variety of industries for the foreseeable future. Thus, practitioners and researchers should continuously seek to work together to understand the dynamics of the ISRA process and improve the methods for its execution.

REFERENCES

Allen, B. (1968). Danger Ahead! Safeguard Your Computer. *Harvard Business Review*, 46(6), 97-101.

Backhouse, J. and Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems*, 5(1), 2-9.

Badenhorst, K.P. and Eloff, J.H.P. (1989). Framework of a methodology for the life cycle of computer security in an organization. *Computers & Security*, 8, 433-442.

Baker, W.H., Rees, L.P., and Tippet, P.S. (2007). Necessary Measures: Metric-driven information security risk assessment and decision making. *Communications of the ACM*, 50(10), 101-106.

Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems*, 1(2), 121-130.

Bodin, L.D., Gordon, L.A., and Loeb, M.P. (2005) Evaluating Information Security Investments Using the Analytic Hierarchy Process. *Communications of the ACM*, (48:2), 79-83.

Brealey, R.A., Myers, S.C., and Allen, F. (2005). *Principles of Corporate Finance* (8th ed.). Boston, MA: McGraw-Hill Irwin.

Bryman, A. and Bell, E. (2003). *Business Research Methods*. New York, NY: Oxford University Press.

Campbell, K., Gordon, L. A., Loeb, M. P., and 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.

Carr, N.G. (2003). IT Doesn't Matter. *Harvard Business Review*, 81(5), 41-51.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004) A Model for Evaluating IT Security Investments. *Communications of the ACM*, (47:7), 87-92.

Commission of the European Communities. (1994). *Europe's Way to the Information Society: An action plan*, Retrieved May 2007, from http://aei.pitt.edu/947/01/info_socieity_action_plan_COM_94_347.pdf

Conry-Murray, A. (2003). Justifying Security Spending. *Network Magazine*, 18(3), 44.

Daft, R. L., & Marcic, D. (2001). *Understanding Management* (3rd ed.). New York: Harcourt College Publishers.

Davenport, T.H. and Prusak, L. (1998). *Working Knowledge: How organizations manage what they know*. Cambridge, MA: Harvard Business School Press.

Detert, J. R., Schroeder, R. G., & Mauriel, J. J. (2000). A Framework for Linking Culture and Improvement in Organizations. *Academy of Management Review*, 25(4), 850-863.

Dutta, A. and McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, 45(1), 67-87.

Gordon, L.A., and Loeb, M.P. (2002a). The Economics of Information Security Investment. *ACM Transactions in Information & Systems Security,* 5(4), 438-457.

Gordon, L.A., and Loeb, M.P. (2002b). Return on Information Security Investments: Myth vs. Reality. *Strategic Finance*, 26-31.

Gordon, L.A., Loeb, M.P., and Sohail, T. (2003). A Framework for Using Insurance for Cyber-Risk Management. *Communications of the ACM*, 46(3), 81-85.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R. (2004). *The 9th Annual Computer Crime and Security Survey.* San Francisco, CA: Computer Security Institute.

Gordon, L.A. and Loeb, M.P. (2006). Budgeting Process for Information Security Expenditures. *Communications of the ACM*, 49(1), 121-125.

Henderson, J.C., and Venkatraman, N. (1993). Strategic Alignment - Leveraging Information Technology for Transforming Organizations. *IBM Systems Journal*, 32(1), 4-16.

Hinde, S. (1998). Recent Security Surveys. *Computers & Security*, 17, 207-210.

Hitchings, J. (1995). Achieving an Integrated Design: The way forward for information security. In Ellof, J. and von Solms, S. (Eds.), *Information Security – the Next Decade*, London: Chapman & Hall.

Holbein, R., Teufel, S, and Bauknecht, K. (1996). The use of business process models for security design in organizations. In S. Katsikas and D. Gritzalis (Eds.), *Information Systems Security: Facing the Information Society of the 21st Century,* London: Chapman & Hall.

Huber, G.P. (1990). A Theory of the Effects of Advanced Information Technologies on Organizational Design, Intelligence, and Decision Making. *Academy of Management Review*, 15(1), 47-71.

International Information Systems Security Certification Consortium, Inc. (2007). *Frequently Asked Questions*. Retrieved December 10, 2007, from https://www.isc2.org/cgi-bin/content.cgi?category=84.

International Standards Organization. (2006). *Information technology—Guidelines for the management of IT security—Part 5: Management guidance on network security*. Retrieved May 2007, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31142

Kankanhalli, A., Hock-Hai, T., Bernard, C. Y. T., & Kwok-Kee, W. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management*, 23(2), 139-154.

Knapp, K., Morris, F., Rainer, R.K., Jr., and Byrd, T.A. (2003). Defense Mechanisms of Biological Cells: A framework for network security thinking. *Communications of the Association for Information Systems*, 12, 701-719.

Knapp, K. J. (2005). A Model of Managerial Effectiveness in Information Security: From grounded theory to empirical test. *Dissertation Abstracts International.* (UMI No. 3201451).

Knapp, K., Morris, F., Rainer, R.K., Jr., and Ford, F.N. (2006). Information Security: Management's effect on culture and policy. *Information Management & Computer Security*, 14(1), 24-36.

Kotulic, A.G. and Clark, J.C. (2004). Why there aren't more information security research studies. *Information & Management*, 41, 597-607.

Lindup, K. (1996). The role of information security in corporate governance. *Computers & Security*, 15, 477-485.

Ma, Q. And Pearson, M. J. (2005). ISO 17799: "Best Practices" in Information Security Management? *Communications of the Association for Information Systems*, 15, 577-591.

May, T.A. (1997). The Death of ROI: Rethinking IT value measurement. *Information Management & Computer Security*, 5(3), 90-92.

Mitnick, K.D. and Simon, W.L. *The Art of Deception: Controlling the Human Element of Security*, Indianapolis, IN: Wiley Publications, 2002.

Moore, M. M. (2003). *Employee Security Education: Pillars of your community*. Retrieved April, 2007, from http://www.csoonline.com/read/010903/pillars.html

OHS. (2002). *National Strategy for Homeland Security*. Office of Homeland Security.

Parker, D. B. (1981). *Computer Security Management*. Reston, Virginia: Reston Publishing Company.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology, 88*(5), 879-903.

Podsakoff, P. M., & Organ, D. W. (1986). Self-Reports in Organizational Research: Problems and Prospects. *Journal of Management*, 12(4), 531-544.

Power, R. (2002). CSI/FBI Computer Crime and Security Survey. *Computer Security Issues & Trends*. 8(1), 1-24.

Ragu-Nathan, B. S., Apigian, C. H., Ragu-Nathan, T. S., & Tu, Q. (2004). A Path Analytic Study of the Effect of Top Management Support for Information Systems Performance. *Omega*, 32, 459-471.

Rainer, R. K, Jr., Snyder¸ C. S., and Carr, H. H. (1991). Risk Analysis for Information Technology. *Journal of Management Information Systems*, 8(1), 129-147.

Rainer, R. K., Jr., Turban, E., and Potter, R.E. (2007). *Introduction to Information Systems: Supporting and Transforming Business*, Hoboken, NJ: John Wiley & Sons, Inc.

Richardson, R. (2007). *The 12th Annual Computer Crime and Security Survey.* San Francisco, CA: Computer Security Institute.

Robey, D., & Boudreau, M.-C. (1999). Accounting for the Contradictory Organizational Consequences of Information Technology: Theoretical Directions and Methodological Implications. *Information Systems Research*, 10(2), 167-185.

Santarelli, S. (2005). *Creating a Corporate Security Culture*. Retrieved May, 2006, from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1137072,00.html

Scandura, T. A., and Williams, E. A. (2000). Research Methodology in Management: Current practices, trends, and implications for future research. *Academy of Management Journal*, *43(6)*, 1248–1264.

Searle, J. R. (1987). *Speech Acts: An Essay in the Philosophy of Language*. New York, NY: Cambridge University Press.

Sharma, R., & Yetton, P. (2003). The Contingent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation. *MIS Quarterly*, 27(4), 533-555.

Simsek, Z., & Veiga, J.F. (2001). A primer on Internet organizational surveys. *Organizational Research Methods*, 4(3), 218-235.

Smith, H. A., McKeen, J. D., and Staples, S. D. (2001). Risk Management in Information Systems: Problems and potential. *Communications of the Association for Information Systems*, 7, 1-28.

Spector, P. E. (1994). Using Self-Report Questionnaires in OB Research: A Comment on the Use of a Controversial Method. *Journal of Organizational Behavior*, 15, 385-392.

Srinivasan, R., Lilien, G. L., and Rangaswamy, A. (2002). Technological Opportunism and Radical Technology Adoption: An application to E-Business. *Journal of Marketing*, 66(3), 47-63.

Stanton, J.M., & Rogelberg, S.G. (2001). Using Internet/Intranet Web pages to collect organizational research data. *Organizational Research Methods*, 4(3), 200-217.

Stoneburner, G., Goguen, A., and Feringa, A. (2002). *Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology.

Straub, D.W. and Welke, R.J. (1998). Coping with Systems Risk: Security planning models for management decision making. *MIS Quarterly*, 22(4), 441-469.

Straub, D. W., Boudreau, M. C., & Gefen, D. (2004). Validating Guidelines for IS Positivist Research. *Communications of the AIS*, 13(24), 380-427.

Suh, B. and Ingoo, H. (2003). The IS Risk Analysis Based On A Business Model. *Information & Management*, 41, 149-158.

Thong, J. Y. L., Yap, C. S., & Raman, K. S. (1997). Environments of Information Systems Implementation in Small Businesses. *Journal of Organizational Computing and Electronic Commerce*, 7(4), 253-278.

von Solms, R., & von Solms, B. (2004). From Policies to Culture. *Computers & Security*, 23, 275-279.

Wasserman, J.J. (1969). Plugging the Leaks in Computer Security. *Harvard Business Review*, 47(5), 119-129.

Weiss, R.S. (1994). *Learning from Strangers: The art and method of qualitative interview studies*. New York, NY: The Free Press.

Whitman, M.E. (2003). Enemy at the Gate: Threats to information security. *Communications of the ACM*, 46(8), 91-95.

Whitman, M.E. and Mattord, H.J. (2003). *Principles of Information Security*. Boston, MA: Course Technology.

Whitman, M.E. and Mattord, H.J. (2004). *Management of Information Security*. Boston, MA: Course Technology.

APPENDICES

Appendix A

Email Blast to the ISRA Survey Phase One Participants

Auburn University - ISRA Survey

Sent out September 18, 2007

Recently, you were kind enough to participate in a research study conducted by Auburn University's Dr. Ken Knapp and Dr. Thomas Marshall. In that study, you indicated that you would be interested in participating in a survey on risk management.

We are currently conducting a study to create a set of best practices for information security risk management. All responses will be completely anonymous and confidential. All results will be reported only in a summarized fashion. No participant information will be revealed. We will be happy to provide you with an executive summary of our results if you would let us know that you would like one.

When you are ready to take the survey, just fill out the Excel spreadsheet attached to this email. Please, begin on the worksheet "Introduction". When you complete the survey, please email the completed spreadsheet to jourdsz@auburn.edu.

It should take between 20 and 30 minutes to complete the survey. Thank you in advance for your participation.

Zack Jourdan
Ph.D. Candidate
Auburn University

APPENDIX B

The Information Security Risk Analysis Questionnaire – Phase One

Survey on Information Security Risk Analysis

1. Introduction

Thank you for your interest in this questionnaire. Through your participation, we hope to learn more about important aspects of information security risk analysis. This survey asks for your opinion about the risk analysis practices of the organization where you currently work or the organization that you support. This survey is on the worksheets (tabs at bottom) named Introduction, Demographics, Threats, Risk Factors, and Risk Analysis.

Prerequisites for taking this survey:
1. You are an information security professional (i.e. CISSP or SSCP). OR
2. You have sufficient experience at the current organization where you work to have an opinion about its risk analysis practices.

Consultants or outsourced employees:
If you divide your time supporting more than one client, answer the questions in relation to the organization where you spend most of your time.

Privacy Statement:
Zack Jourdan is conducting this study. Please, address any questions you may have about this survey to Zack Jourdan (jourdsz@.auburn.edu). Information collected in this study will be part of a dissertation and published in professional journals. Only aggregate results will be published.
"Information obtained in this study identifiable to you will be held in the strictest of confidence. Other than an email address, only general demographic questions will be asked. Your email address will not be shared with anyone. Please participate only once.

All participants will receive a report of the results by email.

Your decision whether or not to participate will not jeopardize your relationship with (ISC)^2 or Auburn University. If you withdraw from this study, we will delete all provided information.

If you agree to participate, please fill out all portions of this survey.

If you do not agree to participate, please forward this file to colleagues who might be interested in completing this survey.

Please, select the best answer from the blue list boxes. Please, type longer answers in the green text boxes.

Please enter your email address.

Please select your certification:
None
CISSP
SSCP
CAP
Other

If you have more than one certification or certifications not in the list, please describe here:

2. Demographics

Instructions:
All questions pertain to the entire organization where you work or the organization that you support. Answering these questions is very important for correct interpretation of the questionnaire results. Please, select the best answer from the blue list boxes. Please, type longer answers in the green textboxes.

How many employees work in this organization?
500 or less
From 501 to 2,500
From 2,501 to 7,500
From 7,501 to 15,000
More than 15,001

Select the country where you perform the majority of your work.
List box of countries

Are you an outsourced (consultant) worker?
NO, I'm a regular/permanent employee.
YES, I'm an outsourced worker.

From the list below, select the primary industry that best describes the organization where you do the majority of your work. (Choose only one.)
Consultant
Government-federal, military, local, etc.
Medical/Healthcare-public or private
Finance, Banking, & Insurance
Professional Services-Legal, Marketing, etc.
Consumer Products/Retail/Wholesale
Education/Training
Energy
Information Technology/Security/Telecom
Entertainment
Industrial Technology
Manufacturing
Non-Profit
Publishing
Travel/Hospitality
Transportation/Warehousing
Utilities
Real Estate/Property Management
Other

If you chose other for industry, please describe the industry where you do most of your work.

Which of the following describes your primary job function?
Owner/Partner
Senior Manager/Executive (e.g. CEO, CIO)
Department Manager/Supervisor/Director
MIS/IS/IT/Technical management
Other Managerial
Consultant/Contractor
Other IT/Technical/Scientific/Professional

How many total years of experience do you have in information technology?
5 years or less
Between 6 and 10
Between 11 and 15
Between 16 and 20
More than 20

How many total years of experience do you have in information security?
5 years or less
Between 6 and 10
Between 11 and 15
Between 16 and 20
More than 20

Is information security a primary or secondary responsibility of your current job?
Primary
Secondary

3. Threat

For each threat listed below, please choose the threats significance to your organization.

Extremely significant	5
Significant	4
Neither insignificant nor significant	3
Insignificant	2
Extremely insignificant	1

Please, choose yes if your organization emphasizes this risk factor and no if your organization does not emphasize this risk factor. Please, respond for each risk factor in the list.

Threat	Example
Act of human failure.	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures of errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technical obsolescence	Antiquated or outdated technologies

4. Risk Factors and Insurance

When developing risk factors for your organization's risk analyses, which factors do your organization focus on the most?
Legal, regulatory, or statutory requirements
Loss of consumer confidence
Damage to organization's image/brand
Financial losses
Risks to infrastructure
Risks of possible lawsuits
Business requirements for information confidentiality, integrity, and availability
Other

If you selected other for risk factors, please describe here:

Describe the main factors that your organization uses to establish acceptable risk levels. What would you add to, delete from, or alter in the above list of factors?

Does your organization calculate Return on Investment (ROI) for information security investments and expenses?
Yes
No

If your company does calculate ROI for information security, please describe how your organization calculates this ROI.

Does your organization purchase insurance to cover its information assets?
Yes
No

As a percentage, how much of your organization's tangible information assets (i.e. physical assets, buildings, equipment, computer hardware, etc.) are covered by insurance? Why did your organization choose that percentage?

As a percentage, how much of your organization's intangible information assets (i.e. profits, temporary operating expenses, intellectual properties, electronic files, databases, proprietary programs, etc.) are covered by insurance? Why did your organization choose that percentage?

5. Risk Analysis

How often is the information security risk analysis conducted for your department within your organization?
Never
Rarely
Annually
Quarterly
Weekly/Monthly
Continuously

How often is the information security risk analysis conducted for your entire organization?
Never
Rarely
Annually
Quarterly
Weekly/Monthly
Continuously

Which of the following individuals at your organization participate in information security risk analysis? Please, choose yes if this individual is involved and no if this person is not involved. Please, answer yes or no for each individual.
Owner/Partner
Senior Manager/Executive (e.g. CEO, CIO)
Department Manager/Supervisor/Director
MIS/IS/IT/Technical management
Other Managerial
Consultant/Contractor
Other IT/Technical/Scientific/Professional
Other employees

At your organization, who is involved in the information security risk analysis process? Please, describe the individuals and their roles here:

Which of the following individuals at your organization have final approval of the information security risk analysis? Please, choose yes if this individual is involved and no if this person is not involved. Please, answer yes or no for each individual.
Owner/Partner
Senior Manager/Executive (e.g. CEO, CIO)
Department Manager/Supervisor/Director
MIS/IS/IT/Technical management
Other Managerial
Consultant/Contractor
Other IT/Technical/Scientific/Professional
Other employees

At your organization, who has final approval of the information security risk analysis process? Please, describe the individuals and their roles here:

1. **Determine IT assets**
2. **Determine value of IT assets.**
3. **Enumerate possible threats to IT assets.**
4. **Determine vulnerability of assets to specific threats.**
5. **Determine risk exposure for organization.**
6. **Minimize exposure and/or purchase insurance to minimize risk exposure.**

Do you agree with the process for information security risk analysis in the above list?
Yes
No

What would you add to, delete from, or alter on this list of steps for information security risk analysis/audit?

Select all information security risk analysis/audit methodologies used at your organization. Please, choose yes if your organization uses this methodology and no if your organization does not use this methodology. Please, answer yes or no for each methodology.

Anti-virus software analysis
Password cracking and improvement
Firewall implementation and correction of configuration errors
Vulnerability testing/correction
War dialing (scanning for unauthorized modems and fax machines)
Identification of critical infrastructure components
Physical security review
Centralized information storage location review
Access control evaluation
Certification identification
Integration of the firewall, VPN and e-commerce
Assessment of the routers and servers
Cryptography review
Computer Security Policy review and documentation
Other

If you selected other for methodology, please describe here:

Describe the combination of information security risk analysis/audit methodologies used at your organization. What would you add to, delete from, or alter the methodologies listed above?

Choose all the methodologies your organization uses to measure the possible loss exposure of information assets. Please, choose yes if your organization uses this methodology and no if your organization does not use this methodology. Please, answer yes or no for each methodology.

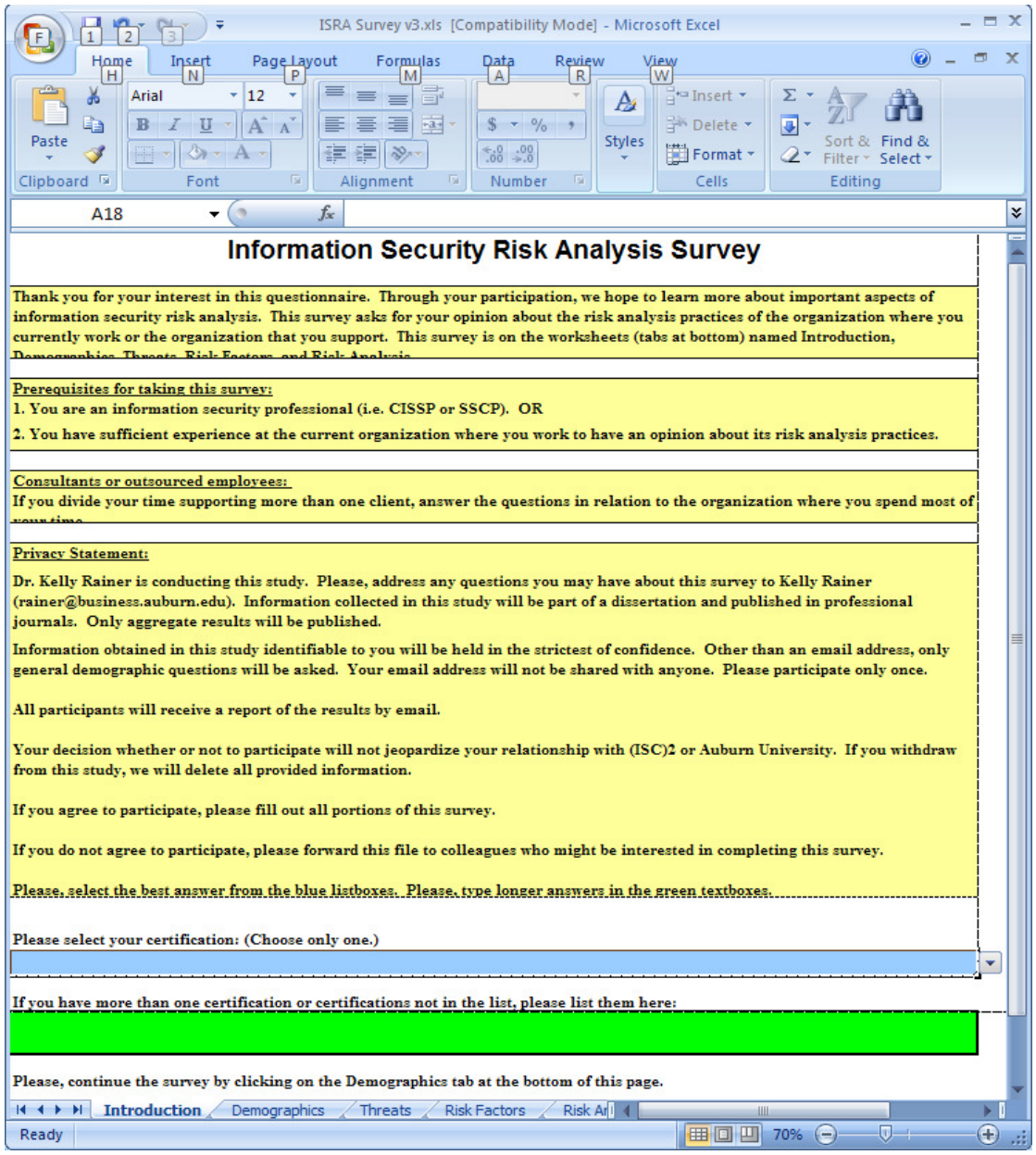
Consultant/Contractor Assessments
Annualized Loss Expectancy (ALE)
Courtney's ALE Method
Cost-Benefit Analysis (CBA)
Annualized Rate of Occurrence (ARO)
Single Loss Expectancy (SLE)
Livermore Risk Analysis Methodology (LRAM)
Stochastic Dominance/Daily Loss Formula
Scenario Analysis
Delphi technique/brainstorming
OCTAVE method
Fuzzy Metrics
Questionnaires
Surveys
Other

If you selected other for methodology, please describe here:

Describe the methodologies your organization use to measure the possible loss exposure of information assets. What would you add to, delete from, or alter in the above list of methodologies?

APPENDIX C

Screen Capture of ISRA Questionnaire – Phase One



APPENDIX D

Email Blast to the ISRA Survey Phase Two Participants

Auburn University - ISRA Survey

Sent out May 31st, 2009

Recently, you indicated that you would be interested in participating in a survey on topics related to information security.

We are currently conducting a study to investigate how organizations conduct their information security risk analysis. This survey contains no questions pertaining to the vendors, techniques, or personnel used by your organization during the risk analysis process. All responses will be completely anonymous and confidential. All results will be reported only in a summarized fashion. No participant information will be revealed. We will be happy to provide you with an executive summary of our results.

When you are ready to take the survey, just click on this link:

Information Security Risk Analysis Survey

You will be taken to a web-based survey. This survey will not collect any personal information including your email address, Internet Service Provider, IP address, MAC address, or any other personal information. If you have any questions about the survey or would like an executive summary of the results, please email jourdsz@auburn.edu.

The survey should take between 15 and 20 minutes to complete. Thank you in advance for your participation.

Zack Jourdan
Ph.D. Candidate
Auburn University

APPENDIX E

The ISRA Questionnaire – Phase Two

Survey on Information Security Risk Analysis

Introduction

Thank you for your interest in this questionnaire. Through your participation, we hope to learn more about important aspects of information security risk analysis. This survey asks for your opinion about the risk analysis practices of the organization where you currently work.

Prerequisites for taking this survey:

1. Your organization conducts a formal information security risk analysis process.
2. You are an information security professional (i.e. CISSP or SSCP). OR
3. You have sufficient experience at the current organization where you work to have an opinion about its risk analysis practices.

Privacy Statement

Zack Jourdan is conducting this study. Please, address any questions you may have about this survey to Zack Jourdan (jourdsz@auburn.edu). Information collected in this study will be part of a dissertation and published in professional journals. Only aggregate results will be published.

This survey will not collect any personal information including your email address, Internet Service Provider, IP address, MAC address, or any other personal information. No information identifying your organization or you will be collected. Please participate only once.

Your decision whether or not to participate will not jeopardize your relationship with Auburn University. If you withdraw from this study, we will delete all provided information.

If you agree to participate, please fill out all portions of this survey.

If you do not agree to participate, please close your browser's window.

Demographics

Instructions:
All questions pertain to the entire organization where you work. Answering these questions is very important for correct interpretation of the questionnaire results. Please, select the best answer.

How many employees work in this organization?
500 or less
From 501 to 5000
More than 5,000

From the list below, select the primary industry that best describes the organization where you do the majority of your work. (Choose only one.)
Consultant
Government-federal, military, local, etc.
Medical/Healthcare-public or private
Finance, Banking, & Insurance
Professional Services-Legal, Marketing, etc.
Consumer Products/Retail/Wholesale
Education/Training
Energy
Information Technology/Security/Telecom
Entertainment
Industrial Technology
Manufacturing
Non-Profit
Publishing
Travel/Hospitality
Transportation/Warehousing
Utilities
Real Estate/Property Management

Which of the following describes your primary job function?
Owner/Partner
Senior Manager/Executive (e.g. CEO, CIO)
Department Manager/Supervisor/Director
MIS/IS/IT/Technical management
Other Managerial
Consultant/Contractor
Other IT/Technical/Scientific/Professional

How many total years of experience do you have in information technology?

How many total years of experience do you have in information security?

Threats

For each threat listed below, please choose the threat's significance to your organization.

Extremely significant	5
Significant	4
Neither insignificant nor significant	3
Insignificant	2
Extremely insignificant	1

Threat	Example
Act of human failure.	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures of errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technical obsolescence	Antiquated or outdated technologies

Does your organization calculate Return on Investment (ROI) for information security investments and expenses?
Yes
No

Does your organization purchase insurance to protect its information assets?
Yes
No

How often is the information security risk analysis conducted for your entire organization?
Once per year or less often
Quarterly/Semiannually
Continuously (i.e. weekly or monthly)

This is a list of information security risk analysis/audit methodologies that are possibly used at your organization. Please, select the methodologies used by your organization.

Anti-virus software analysis
Password cracking and improvement
Firewall implementation and correction of configuration errors
Vulnerability testing/correction
War dialing (scanning for unauthorized modems and fax machines)
Identification of critical infrastructure components
Physical security review
Centralized information storage location review
Access control evaluation
Certification identification
Integration of the firewall, VPN and e-commerce
Assessment of the routers and servers
Cryptography review
Computer Security Policy review and documentation
Consultant/Contractor Assessments
Annualized Loss Expectancy (ALE)
Courtney's ALE Method
Cost-Benefit Analysis (CBA)
Annualized Rate of Occurrence (ARO)
Single Loss Expectancy (SLE)
Livermore Risk Analysis Methodology (LRAM)
Stochastic Dominance/Daily Loss Formula
Scenario Analysis
Delphi technique/brainstorming
OCTAVE method
Fuzzy Metrics
Questionnaires
Surveys

For each statement below, please choose the answer that describes your organization.
Strongly Disagree = SD
Disagree = D
Neutral = N
Agree = A
Strongly Agree = SA

Security culture
In my organization…
Employees value the importance of security.
Security has traditionally been considered an important organizational value.
Practicing good security is an accepted way of doing business.
The overall environment fosters security-minded thinking.
Information security is a key norm shared by organizational members.

Top Management Support
Top Management is interested in the implementation of an Information Security Risk Analysis Process.
Top Management considers an Information Security Risk Analysis Process as important to the organization.
Top Management has effectively communicated its support for an Information Security Risk Analysis Process.

ISRA Effectiveness
Risk analyses are conducted prior to writing new security policies.
Top management is properly informed of vital information security risk analysis developments.
The information security risk analysis program is successful.
The information security risk analysis program protects the organization's information assets.
The information security risk analysis program is thorough.

APPENDIX F

Screen Capture of ISRA Questionnaire – Phase Two