An Investigation Of Organizational Information Security Risk Analysis

Zack Jourdan, Auburn University Montgomery, USA
R. Kelly Rainer, Jr., Auburn University, USA
Thomas E. Marshall, Auburn University, USA
F. Nelson Ford, Auburn University, USA

ABSTRACT

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. To better understand the current state of this information security risk analysis (ISRA) process, this study deployed a questionnaire using both open-ended and closed ended questions administered to a group of information security professionals (N=32). 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.

Keywords: information systems, security, risk analysis, ISRA

1. INTRODUCTION

From the dawn of the information age, technology has advanced rapidly until today where networked computers are almost ubiquitous. The 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).

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). 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).

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, but 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.

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 to determine the ISRA process in the context of the entire organization.

2. LITERATURE REVIEW

The first section of this literature review 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 final section discusses the various ISRA approaches in detail.

2.1 Information Security

Information Security (Information security) 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 Information security Policy as a subset of the IS function's policy (Whitman & Mattord, 2003; Rainer, Turban, & Potter, 2007).

The Information security policy contains detailed plans and procedures for how the department will carry out all of the Information security 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 Information security 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. Information Security Practices (Whitman & Mattord, 2004)

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

2.2 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 Information security.

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). Even organizations that are proactive with respect to information security have reported uncertainty about the thoroughness of their preparations (Richardson, 2007). To accomplish the goal of minimizing risk to information assets with a minimum investment, several ISRA methodologies have been proposed.

2.3 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 quantitative 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 inherent disadvantages of defining risk in vague variables (i.e. low, medium, high, strong, weak, etc.) that do not provide exact dollar values and probabalities (Rainer, Snyder, & Carr, 1991).

3. RESEARCH METHODOLOGY

This research study combines quantitative and qualitative interviewing techniques. 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. Researchers can combine quantitative and qualitative interview techniques in a study (Bryman & Bell, 2003). The following sections provide descriptions of the three methodological steps used.

3.1 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. 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.

3.2 Data Collection

To initiate data collection, an email was sent to 300 CISSPs asking for their participation in a study. Of the 300 individuals contacted, 32 completed the semi-structured survey for a response rate of 10.67%.

3.3 Data Analysis

The sample was 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 Information security 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.

3.4 Sample Characteristics

Table 2 illustrates the diversity with respect to number of employees, type of industry, job position, IT experience, and Information security 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 information security experience with the vast majority being mid-level professionals with between six and fifteen years of experience.

Table 2. Sample Characteristics of 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%
Information security 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%

4. RESULTS

4.1 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 Information security 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 3 shows that many organizations use some or all of the risk factors to plan their respective Information security 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 3. 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%

4.2 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 4).

Table 4. 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%

4.3 Insurance for Information Security

A minority of professionals (see Table 4) 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.

4.4 ISRA Frequency

When asked about the frequency of the ISRA process at their organizations, 25% chose never or rarely for their department and organization. The fact that this many organizations are conducting their ISRA process with such haphazard infrequency is troubling. About half (40.6%) chose annually or quarterly chose either quarterly for their department and organization. The remainder (34.4%) 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.

4.5 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 5.

Table 5. 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%

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 6, 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 6. 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%

5. DISCUSSION

This research paper lays the foundation for further explorations on the topic of ISRA. Through the use of an expert panel an instrument was created to investigate risk factors organizations focus on to decide their ISRA expenditures. An initial investigation of whether organizations calculate return on information security investment or purchased insurance to protect information assets revealed topics that need further exploration. Organizations are conducting an ISRA process using a variety of methodologies on a frequent schedule and management has interest in and control of this process.

5.1 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.

5.2 Implications for Research & Practice

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%. 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.

5.3 Directions for Future Research

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 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. Future studies need to continue the exploration of this research stream to insure that organizations have the most efficient and effective ISRA process possible.

REFERENCES

1. 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.
2. Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems*, 1(2), 121-130.
3. 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.
4. Brealey, R.A., Myers, S.C., and Allen, F. (2005). *Principles of Corporate Finance* (8th ed.). Boston, MA: McGraw-Hill Irwin.
5. Bryman, A. and Bell, E. (2003). *Business Research Methods*. New York, NY: Oxford University Press.
6. 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.
7. Carr, N.G. (2003). IT Doesn't Matter. *Harvard Business Review*, 81(5), 41-51.
8. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004) A Model for Evaluating IT Security Investments. *Communications of the ACM*, (47:7), 87-92.
9. Conry-Murray, A. (2003). Justifying Security Spending. *Network Magazine*, 18(3), 44.
10. Dutta, A. and McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, 45(1), 67-87.
11. Gordon, L.A., and Loeb, M.P. (2002a). The Economics of Information Security Investment. *ACM Transactions in Information & Systems Security,* 5(4), 438-457.
12. Gordon, L.A., and Loeb, M.P. (2002b). Return on Information Security Investments: Myth vs. Reality. *Strategic Finance*, 26-31.

13. 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.
14. Henderson, J.C., and Venkatraman, N. (1993). Strategic Alignment - Leveraging Information Technology for Transforming Organizations. *IBM Systems Journal*, 32(1), 4-16.
15. 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.
16. 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
17. 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.
18. Kotulic, A.G. and Clark, J.C. (2004). Why there aren't more information security research studies. *Information & Management*, 41, 597-607.
19. Lindup, K. (1996). The role of information security in corporate governance. *Computers & Security*, 15, 477-485.
20. 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.
21. Mitnick, K.D. and Simon, W.L. *The Art of Deception: Controlling the Human Element of Security*, Indianapolis, IN: Wiley Publications, 2002.
22. Moore, M. M. (2003). *Employee Security Education: Pillars of your community*. Retrieved April, 2007, from http://www.csoonline.com/read/010903/pillars.html
23. OHS. (2002). *National Strategy for Homeland Security*. Office of Homeland Security.
24. 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.
25. 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.
26. Richardson, R. (2007). *The 12th Annual Computer Crime and Security Survey.* San Francisco, CA: Computer Security Institute.
27. 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.
28. 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.
29. 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.
30. Weiss, R.S. (1994). *Learning from Strangers: The art and method of qualitative interview studies*. New York, NY: The Free Press.
31. Whitman, M.E. (2003). Enemy at the Gate: Threats to information security. *Communications of the ACM*, 46(8), 91-95.
32. Whitman, M.E. and Mattord, H.J. (2003). *Principles of Information Security*. Boston, MA: Course Technology.
33. Whitman, M.E. and Mattord, H.J. (2004). *Management of Information Security*. Boston, MA: Course Technology.