Leadership and Electronic Data Security within Small Businesses: An Exploratory Case Study

Luis O. Noguerol, Robert Branch

University of Phoenix, USA

luisonoguerol@gmail.com,dr.robertbranch@gmail.com

Abstract

As new information technologies occupy an increasing role in our lives, the protection of the electronic data is likewise becoming a necessity. Electronic crime is growing exponentially, affecting not only personal information, but also the survival of companies around the world, especially small businesses. Therefore, organizational leaders need to be aware of existing and emerging risks associated with the newest information technologies to minimize electronic data leakage. The present qualitative exploratory case study reconnoitered the relationship between leadership and electronic data security within small businesses, with the purpose of discovering how non-information technology leaders might influence employees' behavior in small businesses, and make appropriate decisions about the security of electronic data.

Keywords: Business, Electronic Data Security, Information Technologies, Leadership

Introduction

The preservation of data on paper is obsolete due to electronic data storage capabilities (Easttom, 2006). To remain competitive in the 21st century, leaders of organizations must use new information technology (IT) tools for the storage of not only personal data, but also confidential data. Thus, organization leaders quickly adopt new technologies, and the electronic storage of data has become commonplace in many countries (Leilanie Del Prado-Lu, 2005). Information technologies and resources have been the replacement of manual data recording in many institutions and industries, including homeland security, immigration, and health care.

The increased tendency of the storage of data in electronic format combined with increased Internet connectivity and the resultant exposure to cyber criminals has resulted in the development of specific data protection requirements (McAfee, Inc., 2010; Ponemon Institute LLC, 2011). Data storage technologies must include built-in means of data protection, and users who manipulate the data must receive training so these users are fully aware of the risks from the leakage of corporate data to unauthorized individuals. Employees put their companies at risk when they do not follow policies for the security of information (Siponen, Mahmood, & Pahnila, 2009).

Electronic data security affects governments, multinational organizations, small businesses, and individuals around the world. Organizational leaders must be aware of the serious consequences of electronic data leakage. Organizational leaders who are careless in the acquisition and management of electronic data put the company and employees in jeopardy (Northhouse, 2010).

Boltz (1998) claimed that electronic data leakage has the power to have *devastating implications* on an organization. Leaders must exercise care and self-control, to benefit the enterprise, especially in data security (Guinote & Vescio, 2010). Business leaders can influence employees' behavior toward achieving common goals and objectives, specifically in the areas of information technology and electronic data security.

Problem Statement

There is a lack of electronic data security in businesses of all sizes around the world and many of those businesses have been exposed to cybercrime. Electronic data leakage in small businesses is greater than in large organizations (Adamkiewicz, 2005; Baker & Wallace, 2007; Goodwin, 2005; O'Rourke, 2003), because of financial restrictions, occasional inefficient leaders, and poor attention to little problems not directly related to the business.

The specific problem guiding this qualitative exploratory case study is that some non-information technology leaders in small businesses might not be preventing the exploitation or breach of information technology systems by internal information technology users (Greenfield, 2000). Some employees intentionally or unintentionally breach the security of electronic data.

Recent researchers have indicated that, in most cases, electronic data leakage in small businesses is a consequence of inappropriate leadership and inappropriate managerial practices. Leaders make key decisions in organizations, and if the leaders mishandle information technology issues, the leaders threaten the survival of the business (Davies & Hertig, 2008). In the leader-follower dynamic, leaders have direct and indirect

influence on daily business decisions. Per Northouse (2010), organizations of all sizes have emergent leaders who can contribute to electronic data protection through clear communication and strong knowledge of data protection protocols.

The purpose of the qualitative exploratory case study was the discovery of what manner non-IT leaders might influence employees' behavior in small businesses and make appropriate decisions about the security of electronic data. The study was also an exploration of how non-information technology leaders might influence employees regarding electronic data security in small companies. The population of the study was enterprise leaders, non-information technology leaders, stakeholders, and employees who do not belong to the information technology division, and resided in southeastern Florida, specifically in Miami Dade County and its municipalities, including areas in the immediate outskirts of the county's demographic and surrounding areas.

The main research topic in the study was the influence of non-information technology leaders on employees' behavior regarding electronic data security. For the study, the exploratory case study approach was appropriate for the description and analysis of the way leaders influence employees' behavior regarding electronic data security within small businesses. The participants in the study could explain their understandings of the problem and this information sharing was a significant contribution to the investigator understanding of the participants' point of views (Lather, 1992; Robottom & Hart, 1993).

Research Question

This exploratory case study was for the identification and clarification of some practices directly related to the decisions of leaders and managers in the information

technology field when these leaders may reduce or increase the risk of losing valuable electronic data, and to answer the research question. The guiding research question was: "*How do leaders of small businesses influence employees concerning electronic data security at the company level?"*

Theoretical Framework

Through a qualitative study, the researchers discovered in what manner leaders might influence employees' behavior in small businesses as it pertains to IT security. The participants of the study provided appropriate information on how leaders make decisions about the security of electronic data. The research participants also provided data on how non-information technology leaders might influence employees regarding electronic data security in small companies.

Literature Review

The theoretical framework of the current research included two major studies. Gupta and Hammond (2005) highlighted the negative effects of information technology leaders controlling tasks associated with electronic data security in small business environments. Bhattacharya (2008) examined the possible parallelism between electronic data security and leadership styles in the context of small businesses. Bhattacharya further addressed the risks of electronic data leakage from limited budgets and poor user skills.

Previously, researchers such as Bhattacharya (2008) evaluated the role of information technology managers but ignored the potential role of general leadership in electronic data security. Since the late 1980s, there have been many theoretical discussions concerning the positive influence of transformational leadership as a

predictor of good decision-making. Rehman (2011) noted that, in organizations, transformational leaders have more desired qualities as the transformational leader is more effective and is always raising and pushing the organizations performance forward. Per leadership theory, transformational leaders can make informed decisions in fields outside their area of expertise (Bass, 1990).

Many researchers and leaders believe that non-information technology leaders do not possess the required technical skills to make informed decisions in electronic data security. Per Snyder (2012), the fundamental problem with information technology leaders is that they are focused on theoretical and practical issues, but usually lack the indispensable abilities to work well with others. By contrast, non-technical leaders have special skills that facilitate their interaction with dissimilar groups of followers, but they lack technical skills.

Research Method and Design

The qualitative exploratory case study design was appropriate for the study since an understanding or interpreting of a phenomenon from the perceptions and experiences of the participants, not for the researcher to explain and predict specific phenomena or generate and test a theory.

The main goal of this investigation was the discovery of a relationship, if any, between decisions made by non-IT leaders and their employees. The focus was on the protection of the electronic data in a bounded system in Miami Dade County and its municipalities, including areas in the immediate outskirts of the county's demographic and surrounding areas. A case study was the most appropriate research method for the discovery of the data required to answer the research questions (Merriam, 2009; Yin,

2009; and Stake, 2010). In this study, the data came directly from leaders and employees who have access to electronic data at their company as part of their daily job and could provide a meaningful opinion based on their experiences.

Within this qualitative research method, the combined content examination methodology was helpful in the attainment of an understanding of the emerging themes or patterns constructed on the relationship from the collected face-to-face interviews, the electronic survey, and the field annotations from the face-to-face interviews. The data triangulation method was a combination of data from both instruments and the annotations from the face-to-face interviews. Triangulation of the data was to contrast and compare different types of data to ensure that the results were thorough, accurate, and reflected the experiences of the participants.

During analysis, a comparison between behavioral observations and the text in the transcript was helpful for the construction of a deeper understanding of what was stated by the research participants. The behavior displayed by all participants matched their statements. Data triangulation was part of the research effort for the improvement of the validity and reliability of the data, as well as a technique for the reduction of normal personal bias, that exists in qualitative efforts (Patton, 2001; Shank, 2005; Yin, 2009; Stake, 2010). There was a combination of collected data in support of the research themes thus personal notes and observations were important in a comparison with interview responses.

Three instruments were the main procedures for data collection. One of the procedures for data collection was face-to-face interviews with leaders at each organization. Another of the procedures for data collection were the results of an

electronic survey from employees not related to the information technology division. The third procedure for data collection were the annotations made from the observations during the face-to-face interviews.

Conclusions and Recommendations

The participants described their relationships with subordinates and any influential factors related to data security that they experienced.

Thematic Analysis

Included from the results in this study were findings from the face-to-face interviews, electronic survey data, observational field notes, and the existing literature. Included in the results was a suggestion that restricted budgets and inadequate leadership were factors that were indicative of a small business being at an increased risk for data leakage (Adamkiewicz, 2005; Baker & Wallace, 2007; Goodwin, 2005; O'Rourke, 2003). The electronic survey and the interview questionnaire were validated by a panel of subject matter experts who reviewed the instruments for clarity, bias, and readability.

The data from the electronic survey were in two categories: basic knowledge and the role of management, which were supportive of the research themes. To provide meaningful implications and directions for future research, researchers must examine the results of this investigation against results from previous studies. The following discussion includes a thematic analysis of findings from this investigation and existing literature.

Data was loaded into NVivo Version 10 to organize and aid in thematization. The first step was the development of codes. The coding process involved multiple rounds.

Each piece of data had a descriptive name. During the rounds of analysis, there was alteration, combination, and reconfiguration of the data. Upon completion of the coding the subsequent stage involved the sorting of codes into categories. The creation of categories came from the joining of a series of codes with similar meanings and conceptual links (Saldana, 2009).

Insert the Upon the completion of categories, there was the development of themes. Themes represented the broad overall groupings of the coded data and categories. Theme names reflected the information and data together. Descriptions and illustration of the themes included quotes from the data. Table 1 presents the previous supporting research and themes.

Table 1

Previous Supporting Research

Theme	Previous Supporting Research
Development of a positive work environment	Da Veiga & Eloff, 2010; Herath & Rao, 2009; Tipton & Krause, 2007
Relationship with technology	Dinev & Hart, 2006; Knapp, 2009; Puhakainen, 2006; Siponen et al., 2010; Stanton & Stam, 2006
Relationship with IT staff	Jackson-Palmer, 2010; Rosete & Ciarrochi, 2005
Assessment and reaction to security threats	Bossink, 2004; Keebler & Rhodes, 2002
Impact of security policy	Cherniss & Goleman, 2001; Drucker, 2002; Fedor et al., 2006
Organizational deficiencies	Clark, 2012; Gupta & Hammond, 2005; Muller, 2011

Developing a positive work environment.

Study participants described efforts in their organizations for the promotion of positive work environments for the improvement of interpersonal relationships. Improvements of these relationships, especially between managers and subordinates, may have an impact on the employees' likelihood of adhering to company rules, including electronic data security regulations. The electronic survey included information that employees broke several rules by engaging in unsafe activities, such as sharing passwords and connecting from unsecured networks in public places, such as coffee shops. Participants specifically discussed the importance of professionalism, office camaraderie, and employee incentives for improving office relationships and workplace environments.

Previous researchers have also reported the importance of leaders addressing nontechnical components of workplace environments for maintaining the integrity of company electronic data. Tipton and Krause (2007) indicated that healthy work environments are critical for the protection of electronic data. Leaders in information security management often overlook common factors related to nontechnical components of information security; management, these factors can have a significant influence on the effectiveness of an organization's data security strategies.

Organizational structure is not the sole influence of the normative or subjective beliefs held within a company. The culture of an organization has been influenced by the routines of the employees. A key to effective information security management is for leaders to recognize the importance of nontechnical factors, such as workplace

environments and interpersonal relationships, and the inclusion of those factors in an organization's overall information security strategy.

From the analysis of interview data from this study through face-to-face interviews, it is possible that the leaders of the companies represented in this investigation do not pay adequate attention to existing or potential nontechnical problems related to the development of a positive work environment. This fundamental factor can have an impact on information security. To combat information security threats and to ensure the integrity of a company's electronic data, company leaders must implement comprehensive data security approaches. These nontechnical security measures have a significant role in an organization's efforts for the prevention of accidental catastrophes, intentional theft, or leakage of electronic data and electronic data corruption.

Influencing employees' relationships with technology.

The research participants' relationships with technology seemed to be an influence on the value placed on workplace data-security measures by the participants. Many of the interviewed non-IT leaders described distrust in workplace technology, as well as unfamiliarity with existing data-security policies. If employees perceive these attitudes, managers and non-IT leaders may inadvertently undermine the importance of employee compliance with data security regulations.

Data from the electronic survey were supportive of the perception that managers influenced the employees' feelings regarding IT. While nontechnical leaders often demonstrate stronger interpersonal skills than technical leaders, the nontechnical leaders may lack the technical skills needed to ensure data security. Even though the leaders may

not be directly involved in data security, non-IT leaders may underestimate their critical roles in electronic data security.

Research participants indicated a disinterest in information security because the participants felt IT issues were not part of their direct responsibilities. Participants believed information security responsibilities fell on the shoulders of personnel within technology departments and information security divisions. The belief by non IT employees that IT security was not their responsibility may be an explanation of why the results of the electronic survey showed the employees lacked IT and computer knowledge. Such perceptions include a suggestion that the small business leaders, who participated in this research, were poorly informed regarding data security issues and their roles about information security policies and regulation compliance. To maintain the integrity of electronic data, leaders must keep employees informed of security policies and regulations, and monitor compliance.

Leaders may also improve the reliability of information security controls by implementing regular employee trainings regarding IT security. Within the current study, the participants in the electronic survey data indicated that many employees did not remember receiving training regarding security controls. Researchers have indicated that when companies provide consistent training, employees are more likely to comply with company-specific mandates (Dinev & Hart, 2006; Knapp, 2009; Puhakainen, 2006; Siponen et al., 2010).

Employee training plans are critical for leaders to address the human elements of electronic data security associated with incident response. The practice of training the individuals outside the information security sector is not new. To the average user,

leader, or IT administrator, the task may be challenging. Although many benefits exist to leaders training employees on proper information security practices, implementation may be challenging because it can be difficult for leaders to help employees see the value of such trainings. Leaders should still consider incorporating additional forms of training, especially for proper organizational incident response procedures.

Setting the tone for the relationships with IT staff.

An interesting theme from interview data pertained to the relationships between non-IT employees and IT staff members. Participants who expressed negative opinions of IT departments reported that their subordinates felt the same way. The electronic survey data supported this finding and revealed employees were ignorant regarding whom to contact in their IT department for assistance. In general, non-IT leaders expressed low confidence in IT staff, poor experiences with IT departments, and often blamed technical failures on IT personnel. This finding was essential to the research question, as it indicated an important way that non-IT leaders may influence employees' electronic data security behaviors.

If non-IT leaders have the opinion that electronic data security issues are outside the scope of their jobs subordinates may believe their roles in electronic data security are also significantly limited. Diminished perceived value in the importance of electronic data security may have a reduction factor for the likelihood that employees take security measures seriously and comply with those measures. Within research results there was evidence that the non-IT leaders lacked knowledge regarding basic IT knowledge. Rosete and Ciarrochi (2005) asserted that organizational leaders must operate with a high sense of openness, responsibility, and involvement.

Leaders should do their best for the general benefit of their organizations and be willing to take on additional responsibilities to improve organizational achievement. Non-IT leaders may improve employees' behaviors toward electronic data security protection if they are willing to take on a portion of data security responsibilities and convey the importance of such policies to their subordinates. Jackson-Palmer (2010) suggested that organizational success is contingent upon multiple factors, including the integration of advanced information technologies. The research data also included the observation that IT and information security policies may be insufficient unless leaders and employees share the same vision and assume related responsibilities with similar levels of enthusiasm and responsibility.

Assessing and reacting to security threats.

In addition to their opinions and perspectives of IT responsibilities, participants' assessments of potential data security threats may also have an impact on employee behaviors regarding data security. Leaders from the represented companies described their organizations as well protected against possible cybercrimes. In the electronic survey data participants, revealed that, many employees were ignorant of the proper protocol for security regarding sharing passwords and other security measures. These leaders also believed their network infrastructures were secure and that existing company policies were sufficient measures against breaches in data security. This perspective may be problematic because people need to comprehend the existence of risks in order to understand the importance of following information security policies.

When leaders and employees have different expectations regarding IT resources, information security might be perceived by leaders and employees as less important than

other company issues. The lack of a perception of urgency for IT security can potentially lead to disastrous data security situations. In addition, non-IT leaders could place an organization's survival at risk when they make complex decisions outside their areas of expertise. If leaders underestimate potential threats to electronic data security, the leaders could take it upon themselves to make ill-informed decisions. If leaders believe that data security threats are minimal, the leaders may be less inclined to enforce data security measures among subordinates, thus negatively affecting employee behaviors and attitudes toward such regulations.

Evaluating and enforcing security policy.

Most participants expressed negative opinions toward data security regulations, as well as poor understandings of existing controls. The electronic survey data were supportive of this finding. Some employees felt that regulations were invasive to employees' privacy, while other participants contended that employees should be responsible for learning and following company security regulations. Some participants explained that they felt their companies' data security controls were too restrictive.

This negative attitude toward company data-security regulations and controls may have a significant influence on the behaviors of employees. If leaders believe that data security controls are invasive, overly restrictive, or if the leaders simply do not understand the controls themselves, the leaders may be less likely to enforce the controls, thus placing the integrity of a company's electronic data at risk.

Previous researchers have noted the importance of the existence and enforcement of comprehensive data security regulations. A comprehensive, electronic data security plan is critical for the prevention of potential security breaches. Organizational standards

cannot exist without clearly written security regulations. Without clear regulations, employees may act and make decisions as they deem necessary, and when information technologies are involved with a large number of processes at the organizational level, leaders must rapidly assess the possible implications of information misuse to reduce electronic data leakage. Organization leaders must continuously verify and test the effectiveness of information security measures.

Cherniss and Goleman (2001) declared that organizational success depended on information technologies and theoretical preparation, and that leaders must consider the potential risks to IT resources. The findings from this study include suggestions that the existing security policies within the participants' businesses were inadequate. Through their responses, participants indicated a dangerous lack of knowledge among the participants regarding the possible consequences and implications of security breaches, results of which could be catastrophic to a company's reputation, competitiveness, and survival.

Addressing ongoing organizational deficiencies.

A final theme from this study that may relate to managerial influences on the data-security behaviors of employees is organizational deficiency. Study participants identified several organizational issues that may lead to the impairment of productivity and electronic data security issues in a business. Organization leaders must have company standards and regulations to hold employees accountable for their actions.

Business leaders must create those standards and encourage company employees to follow the standards. In addition, employees must fully understand such regulations. Gupta and Hammond (2005) acknowledged that employee misunderstandings of IT

regulations could be the cause of serious problems with electronic data outflow. The electronic survey data from the current study was supportive of this perspective.

Information security breaches are entering the news daily. Leaders must focus on the importance of electronic data use and how to reduce data breaches by instructing and motivating their followers about existent risks and vulnerabilities. The success of any organization relies on the preparation and understanding of top management regarding the appropriate use of information technologies.

Summary of Thematic Analysis

Within technology literature, a negative relationship exists between non-compliance behavior and an end user's security behavior (Theoharidou et al., 2005). Human beings are prone to stress, which can have a negative effect on leaders' abilities to manage information security policies. Because of this reason, organizational leaders must consider employees' technology usage and security behaviors as part of an organization's information security strategy. Stakeholders and information security professionals must determine the most effective approaches for controlling and implementing necessary countermeasures in a timely manner and identify the effects of such behaviors.

Sekaran (2004) addressed the importance that managers assume responsibility for all organizational tasks, even when those tasks do not fall under their direct duties. To make informed decisions, leaders must be motivated and willing to assume ownership of all company problems. Findings from this study include some suggestions that individuals in top management positions must make major efforts to protect electronic assets, assume responsibilities for their roles in company success, recognize that speedy

improvements are necessary for minimizing risks associated with electronic data leakage, understand the importance of educating their employees on basic computer knowledge as well as general IT training, and be more involved in the enforcement of security policies. When asked about their plans to assume more active roles in electronic data protection, none of the participants from this study indicated any intention of doing so.

Because leaders and employees have different expectations regarding IT resources, information security might be designated as less important and lead to disastrous situations. Non-technical leaders could place the survival of an organization at risk by making complex decisions on topics outside their areas of expertise. Leadership skills could be a robust predictor of organizational success, and it was suggested by the participants in the research that academic preparation was insufficient for the optimum operation of IT divisions.

Per Flint (2005), non-expert IT leaders making IT decisions might fail. Research on this theme included information that top management, non-IT leaders, who were interviewed for this investigation were not well educated on topics related to information security. The research participants indicated that managers infrequently verify tasks related to the protection of electronic data, do not pay necessary attention to security policies, and firmly believe their companies are free from internal threats.

Data Triangulation

All data from this study went through the process of triangulation. The comparison of the data from the electronic surveys, themed interviews, and behavioral observations were the parts of the triangulation process. The themes from the interviews were: (a) developing a positive work environment, (b) influencing employees'

relationship with technology, (c) setting the tone for the relationship with IT staff, (d) assessing and reacting to security threats, (e) evaluating and enforcing security policy, and (f) addressing ongoing organizational deficiencies.

The research included an analysis and comparison of the data from the electronic survey to the themes from the non-IT manager interview data. The results included information regarding the non-IT responses to the electronic survey were supportive of the manager responses. The observational data were consistent to the themes of the important influence of employees' relationship with technology and having an impact on the tone of the relationship with IT staff.

Conclusions

Managers and employees have tremendous and unique responsibilities in the protection of electronic data. During this research, the research participants approached the topic of information security from the perspective of leaders for an exploration of influence that small business, non-IT leaders exert toward their employees regarding IT security issues. Participants indicated that leaders could have a significant influence on the electronic data security behaviors of employees.

The results of the electronic survey data included additional comments on this issue. Participants indicated that many employees lack general computer knowledge as well as lacking knowledge of basic IT security procedures. While the results of this research are not generalizable by another researcher, the results may be helpful to small business leaders as the leaders become more aware of related problems and provide direction for minimizing risks associated with the leakage of electronic data.

A few problems related to electronic data security and leadership remain unresolved. One of the problems is the possible association between the particular area in which the study was conducted and other geographical locations. A second problem is that the exact convenience of non-IT leaders making decisions related to electronic data security is still imprecise. A third problem is how the problem is handled in medium or large size organizations, which presents a topic that needs to be explored; the study did not involve contrasting the perceptions of IT leaders and non-IT experts. A fourth problem is the way employees can influence their leaders in terms of electronic data security require more investigation.

There can be important conclusions from the data of this research. Leaders can positively influence employees' data security behaviors by promoting healthy workplace environments and fostering interpersonal relationships. Leaders should also be aware that their negative opinions on issues related to electronic data security could have a significant influence on employees' behaviors. If managers demonstrate a disinterest in electronic data security policies, employees may reflect that attitude and be less likely to follow a company's information security policies.

Similarly, if managers act as if data security issues are not their responsibilities, subordinates may reflect this attitude and treat data protection dismissively. Regarding the central research question: How do leaders of small businesses influence employees concerning electronic data security at the company level? The researchers found that managers who believe that the threats to data security are minimal may also undermine a company's electronic data-protection policies or be less inclined to enforce such regulations. The belief that data security regulations are invasive, restrictive, or a simple

lack of familiarity with such regulations may also make managers less likely to enforce them, thus placing electronic data at risk.

Findings from this research may be meaningful contributions to existing literature on the topic of electronic data security. Prior to this investigation, in similar studies the researchers did not employ a case study approach. This research included provisions for valuable data regarding the relevant perceptions and experiences of small business employees and leaders. The research included results that are contributions to existing leadership theories and provide important direction for future research on electronic data protection, especially in small businesses.

References

Adamkiewicz, S. L. (2005). *The correlation between productivity and the use of information security controls in small businesses*. Dissertation Abstracts International, *66*(03), 1541B. (UMI No. 3167184).

Baker, W. H., & Wallace, L. (2007). Is information security under control? *IEEE Security & Privacy, 5,* 36-44. doi:10.1109/MSP.2007.11.

Bass, B. M. (1990). *Bass & Stogdill's handbook of leadership: Theory, research, and managerial applications* (3rd ed.). New York, NY: Free Press.

Bhattacharya, D. (2008). Leadership styles and information security in small businesses: An empirical investigation. *Dissertation Abstracts International*, *69*(08), A. (UMI No. 3324059).

Boltz, H. J. (1998). *Information security: Serious weaknesses place critical federal operations and assets at risk*. Washington, DC: General Accounting Office (GAO).

Cataldo, A. J., & Killough, L. N. (2003). Is your firm safe from cybersmear? *Strategic Finance*, *84*(7), 34-38.

Cherniss, C., & Goleman, D. (Eds.). (2001). *The emotionally intelligent workplace: How to select for, measure, and improve emotional intelligence in individuals, groups, and organizations*. San Francisco, CA: Jossey-Bass.

Davies, J. S., & Hertig, A. C. (2008). *Theory and practice of asset protection. Security, supervision and management* (3rd ed.). Burlington, MA: Elsevier.

Dinev, T. & Hart, P. (2006). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce,* 10 (2), 7-29.

Easttom, C. (2006). Computer security fundamentals. Upper Saddle River, NJ: Prentice Hall.

Flint, D. (2005). *The users' view of IT projects that fail.* Retrieved from http://my.gartner.com/portal/server.pt?open=512&objID=249&mode=2&PageID=864059&resId=471119&ref=QuickSearch&sthkw=flint+2005.

Goodwin, B. (2005, February 14). Big guns target supply chain threat. *Computer Weekly*. Retrieved from http://www.computerweekly.com/.

Greenfield, D. (2000). Internet misuse at workplace. Retrieved from http://findarticles .com/p/articles/mi_m0EIN/is_2000_Jan_11/ai_58526705

Guinote, A., & Vescio, K. T. (2010). *The social psychology of power*. New York, NY. The Gilford Press.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security, 13*(4), 297.

Haag, S., Cummings, M., & McCubbrey, D. (2005). *Management information systems for the information age* (5th ed.). Boston, MA: McGraw-Hill.

Jackson-Palmer, J. (2010). The influence of leaders' emotional intelligence on employee motivation. *Dissertation Abstracts International, 71*(10), A. (UMI No. 3425614).

Jaques, R. (2011, May 20). Data breaches more likely to come from within. *Financial Director*. Retrieved from http://www.financialdirector.co.uk/.

Katz, J. (2007, January). Intellectual property: Feeling a little insecure? *IndustryWeek.* Retrieved from http://www.industryweek.com/.

Khosrow-Pour, M. (2006). *Emerging trends and challenges in information technology management*. Hershey, PA: Idea Group.

Knapp, J. (2009). Shakespeare only. Chicago: University of Chicago Press.

Lather, P. (1991). Getting smart: Feminist research and pedagogy with/in the postmodern. New York: Routledge.

Laudon, K. C., & Laudon, J. P. (2006). *Management information systems: Managing the digital firm* (9th ed.). Upper Saddle River, NJ: Pearson Education.

Law, K. S., Wong, C. S., & Song, L. J. (2004). The construct and criterion validity of emotional intelligence and its potential utility for management studies. *Journal of Applied Psychology, 89,* 483-496.

Lehrman, Y. (2010). The weakest link: The risks associated with social networking websites. *Journal of Strategic Security, 3*(2), 63-72. doi:10.5038/1944-0472.3.2.7.

Leilanie Del Prado-Lu, J. (2005). *Gender, information technology, and health*. Quezon City, Philippines: The University of the Philippines Press.

Lester, D. L. & Parnell, J. A. (2006). The Desktop Manager. *S.A.M. Advanced Management Journal*, *71*(4), 43-49, 3. doi: 1197128771.

McAfee, I. (2010). *A good decade for cyber crime.* Retrieved from http://www.mcafee. com/ca/resources/reports/rp-good-decade-for-cyber crime.pdf.

Merriam, S. B. (2009). *Qualitative research: A guide to design and implementation.* San Francisco, CA: Jossey-Bass.

Northouse, P. G. (2010). *Leadership: Theory and practice* (5th ed.). Thousand Oaks, CA: Sage.

O'Rourke, M. (2003). Cyber attacks prompt response to security threat. *Risk Management, 50*(1), 8.

Patton, M. Q. (2001). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34, 757-778. Retrieved from http://www.misq.org/skin/frontend/default/

Rehman, R. (2011). Role of emotional intelligence on the relationship among leadership styles, decision making styles and organizational performance: A review. *Interdisciplinary Journal of Contemporary Research in Business, 3*(1), 409-416.

Robottom, M., I. & Hart, P. (1993). Research in environmental education: Engaging the debate. Geelong, Victoria: Deakin University Press.

Rosete, D., & Ciarrochi, J. (2005). Emotional intelligence and its relationship to

workplace performance outcomes of leadership effectiveness. *Leadership & Organization Development Journal, 26*(5), 388-399.

Saldaña, J. M. (2009). *The coding manual for qualitative researchers*. Thousand Oaks, CA: Sage Publications, Inc.

Sekaran, U. (2004). *Organisational behaviour: Text and cases* (2nd ed.). New Delhi, India: Tata McGraw-Hill Publishing.

Singh, A., & Gilhotra, R. (2011). Data security using private key encryption system, Based on arithmetic coding. *International Journal of Network Security & Its Applications*, *3*, 58-67. doi:10.5121/ijnsa.2011.3305.

Siponen, M., Mahmood, M., & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, *52*(12), 145-147.

Snyder, W. W. V. (2012). Experiences of new information technology managers: A qualitative hermeneutic phenomenological study of IT managers. (University of Phoenix). *ProQuest Dissertations and Theses,* 125. Retrieved from http://search.proquest.com/docview/1015340141?accountid=35812. (1015340141).

Stake, R. E. (1995). *The art of case study research.* Thousand Oaks, CA: Sage Publications.

Stang, J. D. (1992). *Microcomputer security* (6th ed.). Washington, DC: International Computer Security Association. Diane.

Stanton, M. J., & Stam, R. K. (2006). *The visible employee: Using workplace monitoring and surveillance to protect information assets without compromising employee privacy or trust.* Medford, NJ: Information Today.

Straub, Jr., D. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*, 255-276. Retrieved from www.ebscohost.com/academic/business-source-complete.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472-484.

Tipton, F. H., & Krause, M. (2007). *Information security management handbook* (6th ed.). Boca Raton, FL: Taylor & Francis Group.

Van Rooy, D. L., & Viswesvaran, C. (2004). Emotional intelligence: A meta-analytic investigation of predictive validity and nomological net. *Journal of Vocational Behavior*, *65*, 71-95.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM*, *46*(8), 91-95. doi:10.1145/859670.859675.

Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Thousand Oaks, CA: Sage.

Appendices

Appendix A: Proving Interview Questions

1. Talk about the adequacy of your security policies.
2. How have employees understood the risks associated with electronic data leakage?
3. Can you tell me a bit about senior management and its employee engagement on information security?
4. Discuss a time you took a risk with your responsibilities at the office.
5. In an ideal world, how would the top four positions at your company look, and what would responsibilities be?
6. Could you discuss your daily routine with respect to electronic data leakage?
7. Please describe your perception, as part of the management, of your company's security policies and protection of electronic data?
8. What would an ideal plan for protection of your company's electronic assets look like?
9. Given the opportunity to develop a new information security plan for your organization, what activities would you prioritize? How would you minimize the risks associated with electronic data leakage?
10. Can you familiarize me with an online resource I might use to keep up-to-date about the latest news related to the protection of electronic data?
11. Discuss the importance of protecting electronic data in your company, and its ranking in corporate priorities.
12. How do you react to stories about hackers and electronic fraud?

13. What is your perception of the corporate response to the implementation of a new monitoring system in your organization that allows the information technology department to gain full access to your e-mail and Web-browsing activities?
14. Describe the process of implementing a new set of security policies to improve the protection of electronic data.
15. How well do you sleep at night when you think about the security of corporate data?